CYBER CRIME CHANGING SCENARIO

Proliferations

- The release rate of malicious code and other unwanted programs may be exceeding that of legitimate software applications.[1]
- A single threat infected 600,000 Macs in 2012.[2]
- Cybercriminals are doing their homework, and are aware of what's popular, and what's insecure.[3]
- Malware samples in 2012 and now catalogued 100,000 new malware samples each day — that's 69 new pieces of malware a minute. Compared with 60K new viruses average per day in 2010.[4]
- As much malware produced in 2007 as in the previous 20 years altogether.[5]
- Detection rates for threats had dropped from 40-50% in 2006 to 20-30% in 2007.[6]
- Anti-Virus solutions do not provide adequate protection even a month after new malware threats have been detected.[7]
- Malware's most common pathway from criminals to users is through the Internet; primarily by e-mail and the World Wide Web.[8]
- One in every 14 downloads from the Internet may now contain malware code.[9]
- Many virus scanners produce false positive results as well, identifying benign files as malware.[10]

Citations

1. Symantec Internet Security Threat Report: Trends for July–December 2007 (Executive Summary)
2. Symantec: 2013 Internet Security Threat Report, Volume 18
3. Mike Gallagher, senior vice-president and chief technology officer of Global Threat Intelligence for McAfee
4. McAfee: Infographic: The State of Malware 2013
5. F-Secure Reports Amount of Malware Grew by 100% during 2007
6. Computer Magazine c't found
7. Malware Detection Rates for Leading AV Solutions A Cyveillance Analysis August 2010
8. F-Secure Quarterly Security Wrap-up for the first quarter of 2008
9. Microsoft reported in May 2011
10. AV Comparatives (December 2013). "Whole Product Dynamic "Real World" Production Test"

CYBER CRIME CHANGING SCENARIO

Before proceeds, we should know functioning of anti-virus programs:
The Antivirus Program employed Signature and Heuristic Based system for the Detection Process.

- **Signature based Detection** compares the contents of a file to a dictionary of virus signatures. Means thereby *Signature-based detection involves searching for known patterns of data within executable code.*
- **Heuristic-based detection** used to identify unknown viruses by looking for slight variations of known malicious code in files.

If the antivirus software employs heuristic detection, it must be fine-tuned to minimise misidentifying harmless software as malicious (false positive).

Analyse on the above method:
Signature based approach will be used where the virus/ malware program has been identified and knows the affect of their working. In heuristic system of approach only prediction process of permutation and computation method is followed.

Series No. I: Let us discuss the following examples:

- Mr X developed a program for himself and decides, if someone tries to access the same, the embedded program will start destroying the files of the unauthorised user system.
- Mr X developed a program for himself and decides, if someone tries to access the same, the embedded program will start destroying the files of the embedded program itself.
  In both the above examples the code for destroying the files are same.

Now, analyse the issue:

- If Mr. X program is not for others, then Mr. X is an only user for that Mr. X should secure its program rather to destruct others system. In later example Mr. X is restricting the use of the program from unauthorised access.
- Now think, if the same code is used by some other programmer and is detected by anti-virus software organisations. The same code is used by anti-virus software organisations for further detection and destroying the effectiveness of the same code for legitimate purpose.

In conclude with, there are no methods/ procedures to identify the difference between the legitimate and malicious intentions; hence this is a limitation for antivirus programs.

CYBER CRIME CHANGING SCENARIO

Series No. II: Let us discuss the following example:

- Intruder developed a program with malicious intention using new technique.

Now, analyse the issue:

- Before destroying/ restricting use of malicious code, the protector should determine
  - First identify that the program is a malicious code,
  - Then find the instructions/ techniques used in the malicious code, and
  - Finally develop the anti-code for malicious code,
- For the above process, the protector required skills better than the intruders.

In conclude with, the protector required a skill/ knowledge better than the malicious code programmer.

CYBER CRIME CHANGING SCENARIO

How antivirus programs defend from the following activities?

- Where malicious programs routinely defend themselves against removal, not merely to hide themselves?

  It is a very critical issue and arguable, in respect with where defender/ protector faces the issue to recover itself. Where malicious code restricted the use of security program/ code, then defender is not able even to detect the malicious code.

  Currently the intruder's developing the code for restriction the working/ use of the security programs for their effective use for malicious purpose.

  With changing face of technology and awareness of intruder's, now a days intruder's coding the program not merely to hide but also to fight with anti-code and establishing restriction thereon.

  The antivirus software organisation are required to fight with them in advanced manner, by using the philosophy of: to catch the thief, use brain as thief.

  How to defend against new and unknown malware where signatures have not been created or installed?

  The anti-virus/ malware developer are using both the methodologies- signature and heuristic based system of detection, but both are having their side effects, therefore only anti-virus is not able to protect user.

  The user is required to take further steps for security such as VPN services of ISP and Firewall to restrict unauthorised access, etc.

  For clarification: *According to The New York Times, a Symantec customer, reported today that its computer network was hacked repeatedly by attackers in China, and that Symantec's programs didn't catch the breaches. In response, Symantec put out a statement that said "**anti-virus software alone is not enough.**"*

- How to segregate legitimate intended written code from malicious code, i.e. the issue related to false positives?

  Any program executes only on its activation, program doesn't knows to whom he is performing, it always works on based of pre-defined information, hence thereby program itself can't segregate the legitimate program from malicious code.

  Centralised Agency can control the issue in the following manner:

  - Every Developer or Developing Organisation shall has to register
  - After each Development or change in program shall get its approval
  - The Centralised Agency shall issue an code which shall be registered with the program
  - The Centralised agency shall allowed only one unique internet explorer to control and monitor with program or sites runs thereon.

CYBER CRIME CHANGING SCENARIO

- Where malware modified/ changed its signature without affecting its functionality?

  There are several issue and if you recall that every time intruder breaches the security to access data from the database, such as ids, security codes of one sites or organisation in similar manner.

  While any security breaches, the organisation work on the method which they had adopted and similarly work on the same to protect from similar attach without changes the whole system, simultaneously intruder identify further methodology to penetrate again.

  All of the activities are feasible due to the vulnerability has been found by the intruder.

  The organisation are required to control their internal working, with the help of professionals who are expert in designing internal control mechanism, especially finding ways.

- How to protect systems [recover itself] where malware restricts the effectiveness of the anti-virus/malware?

  It is further a critical issue, because it is a process of recovery, and its amount to loss of working. The user are required on the basis of data criticality decides the recovery objective and their time to recover.

  In process of recovery- there are several aspects before the user, but user are required first it's survival.

  Once again, the user shall not depend only on anti-virus for security concern, but also has to use- secured network, approved/ authorised and licenced programs of third party, to protect somehow.

- Is there any algorithm that can perfectly detect/ protect all possible viruses/ attacks?

  Before to given remark, I am remembering one Dr. CA Girish Ahujaji,

  One day on impressed on working of our honourable Ex-Prime Minister, God says, Indira you may ask three questions, I will give you reply on the same:

Indira Asked I	When Sanjay Gandhi becomes Prime Minister of India
God Replies	he has no more life
Indira Asked II	When Rajiv Gandhi becomes Prime Minister of India
God Replies	you have no more life
Indira Asked III	When Taxation become simple in India
God Replies	Not in my life

  In same, the anti-virus/ malware organisation are having limitations because different program, different platforms, different programming languages, different programmer hence not possible at all.

  There is no perfect algorithm to detect, control over malwares/ virus.

CYBER CRIME CHANGING SCENARIO

In Nutshell:

The perpetrator is penetrating by using vulnerabilities and accessing system through port via communication media.

The Protector always tries and gives protection to the best of their working.

The user always focused on the working by keeping in mind that, I am using the shield of protection of anti-virus organisation, secured environment, secured network devices, etc. but he forgets the basic principal- without hole in the system nobody can move.

IT MEANS THE USER HAS TO ALERT AND TAKE PRECAUTIONS WHILE ESTABLISHING SECURED ENVIRONMENT.

CYBER CRIME CHANGING SCENARIO

Now analyse Perpetrators' Intentions by way of some questions as without knowing intention of perpetrators we can't move towards our objective

LET ANALYSE

Time and Money	any executable code require deep analysis to design and write program hence for analyse requires time and every code can only be written by using system infrastructure that require money/ investment.
Harmful to Us	where executable code gather information relates to user or restrict our services or tempering system.
Thinking in Affirmative Manner	where the intention is clear and in favour of user.

NOW THINK ON GENERAL BEHAVIOUR OF USER

- Requires each and everything whether useful or not,
- Don't want to pay anything in any manner, in other words free,
- Want each and everything ready to use in quick time (means whatever they requires that should be available like provided by Jin to Aladin),
- Want to easy to use i.e., user friendly environment, in other words he doesn't want to do by itself
- Doesn't control over own activities

1. Why are they wasting time and money?

   Because they penetrate by affecting their working, or gaining benefit over user information and money, etc.

2. Why are these harmful?

   Because they in unauthorised manner gaining access over system or breaches security, hence user working affects and leads to harmful.

3. Why they are not using their energies in a positive manner?

   Always circumstances leads to malicious intentions, hence, without knowing the facts no-one can conclude even statement.

Somehow, the perpetrator has malicious intention, or ego satisfaction, and situation/ condition arises for do alike, in all the aspects the user always facing the issues such as for security, protection or recovering the data in all terms security providers always in benefit by selling their products.

I am not expecting that, no-one in world wants to call or recognised as thief or destroyer, etc. because nobody wants to gets penalised and punished thereon.

Perpetrator are required to compete with the professionals in affirmative manner and I am sure they will perform far better than the performance of the professionals.

In same way, I am requesting to all personals that if you can't promote someone then you should not demoralise someone.

CYBER CRIME CHANGING SCENARIO

More Serious Issues

1. Is human life secure?

   No, because the penetrator access NASA system which researched and worked for SPACE, which was hacked and instructed as per instruction of intruder instead of highly security, then how we are secure.

2. Whether malware impacts organisations' existence?

   Yes, there are numerous case studies, you may refer Ken Allan, London, 29 October 2013- EY Global Information Security Leader adds: **"Cyber-crime is the greatest threat for organizations' survival today."**

3. Whether Security Provider are themselves secure?

   No, hacking is feasible at almost everywhere as mentioned in proliferation.

4. Does legitimate software have vulnerabilities?

   Yes, vulnerability refers to identification of risk, and based on facts of the cases such as NASA, FBI, CBI, wikileaks, etc., almost all software has vulnerabilities.

5. Whether patches for coping with vulnerabilities are released before threat?

   Yes, but in some case before installing patches by the user the intruder find vulnerabilities to penetrate.

6. Whether all malwares are identifiable?

   No, in most cases for reputational factor, and other detection factor.

7. Whether detection of malware really matters?

   Detection and restriction both are different, in detection only reportable and in restriction to restrict the effectiveness. Hence, detection just a trigger, if not restrict thereupon it will work as instructed by the intruder. Therefore, detection matters where actions for restriction are available.