Malicious Software

Chapter # 06

Date: _____

→ Malicious s/w or malware ⇒ "a program that is inserted into a system, usually covertly, w/ the intent of compromising CIA of victim's data, apps or OS, or otherwise annoying or disrupting the victim's."

Types of Malicious Software (Malware)

→ Advanced Persistent Threat (APT) :- prolonged and targeted attack in which intruder remains undetected in the n/w for an extended period of time. It is initiated to steal info rather than cause damage. Hackers typically ~~target~~ selects. high-value targets such as political parties, nation-states, & large corporations.

→ Adware :- pop-up ads or redirection of a browser to a commercial site.

→ Attack Kit :- set of tools for generating new malware automatically using a variety of supplied propagation & payload mechanisms.

→ Auto-Rooter :- malicious hacker tools used to break into new machines remotely.

→ Backdoor (Trapdoor) :- any mechanisms that bypasses a normal security check; it may allow unauth access to functionality in a program, or onto a compromised system.

→ Downloaders :- normal looking programs designed to fetch and install malware w/o raising any security alarms.

→ Drive-by-Download :- unintentional download of malicious code to your comp or mobile (you don't have to click on anything, press download, or open a malicious email to become infected). Attack client when a site is viewed. Ex: eg- a post on social media feed that is masked to look as though it was sent from sources you trust. This social engineering tactic is used to entice you to click & open. Once the website is open, the driven by download installs itself.

Date:

→ Exploits :- takes advantage of a particular vulnerability (can be one or multiple)

→ Floodors (DoS client) :- Attacker floods a specific target w a massive amount of traffic & data. by carrying out some sort-of DoS attack.

→ Keyloggers :- captures keystrokes on a compromised system.

→ Logic Bomb :- code inserted into malware by an intruder. Lies dormant until a predefined condition is met; the code then triggers some payload.

→ Macro Virus :- written in macro lang, embedded in a doc or doc templat, and triggered when the doc is viewed or edited, to run & replicate itself into other such doc. Targets s/w rather than systems & can infect OS.

→ Mobile Code :- s/w that can be shipped unchanged to heterogeneous collection of platforms & execute w identical semantics.

→ Rootkit :- set of hacker tools used after attacker has broken into a comp sys & gained root-level access.

→ Spammer Programs :- used to send large volumes of unwanted e-mails.

→ Spyware :- s/w that infects comp & other internet-connected devices & secretly records your browsing habits, the websites you visit, & your online purchases. It secretly gathers data/info about a person or org & relays this data to other parties.

Date: _____

→ Trojan Horse :- conceals its true contents to fool a user into thinking its a harmless file.

→ Virus :- type of comp prog that, when executed, replicates itself by modifying other comp programs & inserting its own code. If this replication succeeds, the affected areas are then said to be "infected".

→ Worm :- standalone malware prog that replicates itself in order to spread to other comp. It often uses a comp n/w to spread itself, relying on security failures on the target comp to access it. It will use this n/w to scan & infect other comp.

→ Zombie, Bot :- a comp connected to the internet that has been compromised by a hacker via a comp virus, worm, trojan horse prog and can be used to perform malicious tasks under the remote direction of the hacker.

→ malware can be classified into 2 broad categories :- (check slide#04)
i- how it spreads or propagates to reach the desired targets.
ii- actions or payloads it performs once a target is reached.

→ Propagation mechanisms include infection of existing executable or interpreted content by viruses that is subsequently to spread to other systems.

→ Payload actions performed by malware include corruption of sys or data files, theft of service in order to make the sys zombie, theft of info like logins, passwords, or other personal details by keylogging or spyware.

Date:

→ early malware → single means of prop & single payload.
→ now → blended malware → range of both prop & payloads

• Blended Attacks:- use multiple methods of infection or prop to maximize the speed of contagion & the severity of attack.
(update mech → change range of prop & pay once its deployed)

• Attack Kits:- also called "crimeware", include variety of prop & pay that even novices can combine, select, & deploy. Can be easily customized
Less sophisticated - but can be used to create new large no. of variants..
Eg ①:- Zeus crimeware toolkit, used to generate wide range of very effective stealthed malware. (particularly capturing & exploiting banking credentials)
Eg ②:- Angler exploit kit, first seen → 2013, most active → 2015, advance in both attacks & resistance against detection. ~~of~~ counter-measures.

• Attack Sources:- ~~polit~~ politically motivated attackers, criminals, & organized crime org that sell their services to companies & nations, & govt agencies.
↑motivation behind rise of malware, sale of attack kits, access to compromised hosts etc.

~~Advanced Persistent Threat (APT)~~

Propagation - Infected Content - Viruses

• sfw fragments, that attach themselves to some existing executable content.
↳ may be mlc code or
code used to boot a comp sys
~~majority of malware~~
• recently fragment. has been some form of script code, used to support active content w/in data files such as ~~Microsoft~~ MS Word doc, Excel sheet, or Adobe PDF doc.

Date: _____

→ a comp virus is a piece of code that can "infect" other progs, or indeed any type of executable content by modifying them. Modification included injecting the original code w/ a routine to make copies of the virus code, which can then go on to infect other content.

→ First appeared → 1980s., termed by → Fred Cohen
→ Brain virus → 1986 → first to target MSDOS sys

• Similar to how biological virus tricks living cell into making thousands of replical of original virus, the comp virus carries the code recipe for making perfect copies of itself.
• Virus first embeds in a prog, in a comp, then wherever ~~or a system of or~~ the infected comp comes in contact w/ an uninfected piece of code a fresh copy of virus passes into new location. (This is how it spreads)

→ One reason viruses dominated earlier → lack of user auth & access control. Then macro viruses came into play, they exploit active content supported by some doc types, such as Word, Excel, Adobe etc. Such doc are easily modified & shared and are not protected by same access control as other programs.

→ 3 Parts of Computer Viruses-

i- Infection Mechanism:- means by which a virus spreads or propagates, enabling it to replicate. Also called "infection vector".

ii- Trigger:- event or cond that determines when the payload is activated or delivered. Also called "logic bomb".

Date:

iii - Payloads - what the virus does, besides spreading. May involve damage or may involve benign but noticable activity.

- 4 Phases of Viruses -

i - Dormant Phase :- idle, eventually activated by some event (like date), presence of a/c prog or file, or capacity of disk exceeding some limit. Not all viruses have this stage.

ii - Propagation Phase :- virus places a copy of itself in a/c prog or certain sys areas on the disk. Copy may not be identical as viruses often morph to evade detection. Copy further propagates.

iii - Triggering Phase :- virus is activated to perform the func for which it was intended. Happens after an event like how many copies has the virus made etc.

iv - Execution Phase :- function is performed. (can be harmless or destructive)

→ most viruses take advantage of system's weaknesses, however macro viruses target specific doc types.

Propagation - Vulnerability Exploit - Worms

- a worm is a prog that actively seeks out more m/c to infect, infected m/c then attack other m/cs. Worms prog exploit vulnerabilities in client or server prog. to gain access to each new sys. Use n/w conn to spread can also spread through shared media (USB, CD, DVD)
- Email worms spread in macro or script code included in doc attached or to instant msg file transfers. Upon activation, worm may replicate & prop again. Worm prop + carry payload.

Date:

• comp worm → John Brunner's → 1975 → SF novel The Shockwave Rider
• first know worm implementation → Xerox Palo Alto Labs → 1980s early.
It was not malicious, searching for idle sys to use to run computationally intensive tasks.

→ To replicate itself worm uses some means to access remote sys like:-

1- Electronic Mail or Instant Messenger facility:- worm emails copy of itself to other sys, or sends itself as an attachment via an instant message service, so that its code is run when the email or attachment is received or viewed.

ii- File Sharing:-
iii- Remote Execution Capability:-
iv- & File Access or Transfer Capability:-
v- & Login Capability:-
} pg# 216

→ worm has same phases like virus wer prop phase performs following funcs.
i- search for appropriate access mechanisms on other sys to infect.
ii- use the access mechanism found to transfer a copy of itself to the remote sys and cause the copy to run.

→ worms can determine whether a sys has previously been infected, or disguise its presence by naming itself as sysB proc, & can even inject their code into existing procs on the sys.
(pg# 217 - 219)

Date: _____

→ The Morris Worms-

- Robert Morris, 1988., designed to spread in UNIX sys., used diff prog tech. When a copy began exe, 1st task → discover other hosts known to this hosts. Then for each discovered host, the worm tried a no. of methods for gaining access. (pg# 129).

→ History of Worm Attacks :-

i- Melissa :- email worm; 1988; make use of MS Word macro embedded in an attachment. If recipient open email attachment, macro is activated & it,
→ sends itself to everyone on user's mailing list
→ does some local damage
→ if trigger time was seen, it displayed a Simpson quote as its payload.

→ July 1999 → more powerful version of this. Could be activated merely by opening the email. Melissa prop as soon as its activated whereas viruses take months or years. It took only 3 days to infect over 100,000 comps compared to months took by Brain virus. to infect thousand comp.

ii- Code-Red :- July 2001, exploits security hole in MS IIS to penetrate & spread. Disables sys file checker on Windows. Probes random IP addr. to spread. During certain period it only spreads & then launches a DoS against a govt website by flooding the website w/ numerous pkts from diff hosts.. Code Red infected nearly 360,000 servers in 14 hours in second wave.

iii- Code-Red-II :- August 2001, tried to infect sys on the same subnet. Installs backdoor, allowing a hacker to remotely exe commands on victim's comp.

Date:

iv- Nimda :- September 2001, has worms, virus, & mobile code characteristics using emails, windows shares, web servers, web clients, backdoors (pg# 220)

v- SQL Slammer :- early 2003, exploited buffer overflow vulnerability in MS SQL server. Extremely compact & spread rapidly, infected 90% hosts within 10 mts.

vi- Sobig.F :- late 2003, exploited open proxy servers to turn infected m/c into spam engines, accounted more than 1 million copies of itself within first 24 hrs.

vii- Mydoom :- 2004, mass-mailing email worm, installing backdoor in infected comp.'s, replicated upto 1000 times per min & flooded the internet w/ 100 million infected msgs in 36 hrs.

viii- Warezov :- 2006, when worm is executed/launched it executes several executables in sys directories, sends itself as an email attachment, capable of downloading other malwares & disabling security related products.

ix- Conficker (or Downadup) :- November 2008, massive widespread infection after SQL Slammer. Exploits windows buffer overflow, could also be spread via USB & n/w file shares.

x- Stuxnet :- 2010., deliberately restricted its rate of spread to reduce its chance of detection. Targeted industrial control sys (pg# 221)

xi- Duqu :- late 2011, code related to Stuxnet. aim is diff.

xii- Flame Family :- 2012, target Middle-Eastern countries.

Date:

→ WannaCry Ransomware Attack :- May 2017.

spread extremely rapidly over a period of hours to days, infecting 100's of 1000's of sys belonging to both public & private org. in more than 150 countries. It spreads as a worm by aggressively scanning both local & random remote n/w, to exploit vulnerability in SMB file sharing service on unpatched Windows sys.

→ Rapid spread accidentally slowed thru activation of a "kill switch" domain by a UK security researcher.

→ It also encrypt files, demanding a ransom payment to recover them.

→ State of Worm Technology :-

i- Multi-platform :- newer worms are not limited to windows m/c but can attack other platforms like Unix or exploit macro/scripting langs in doc types.

ii- Multi-exploit :- penetrate using exploits against Web servers, browsers, emails, file sharing, & other n/w based apps, as vs shared file models.

iii- Ultrafast Spreading :- exploits various techniques to optimize the rate of spread.

iv- Polymorphic :- evad detection, skip past filters, & foil real-time analysis, each copy of the worm has new code generated on the fly.

v- Metamorphic :- in addition to changing their appearance, metamorphic worms have collection of behavior patterns that are unleashed at diff stages of prop.

vi- Transport Vehicles :- used for spreading wide variety of malicious payloads, such as bot DoS, rootkits, spam email generators, and spyware.

Date:

W- Zero-day Exploit:- attack targetting a sfw vulnerability unknown to the sfw vendor or to antivirus vendors. In 2015, 54 zero-day exploits were discovered & exploited.

→ Mobile Code:-

mobile code is transmitted from a remote sys to a local sys then exe on local sys w/o user's explicit instruction. Takes adv of vulnerabilities to perform its own exploits such as unauthorized access or root compromise.

- Popular vehicles → Java applets, ActiveX, JavaScript & VB Script.
- Common methods for w/o MC on. & on local sys → cross-site scripting, interactive & dynamic websites, email attachments, downloads from untrusted sites / sfw.

→ Mobile Phone Worms:- (MPW)

- due to Cabir worm: 2004 & then Commwarrior & Lasco: 2005.
- these worms comm thru BT or MMS. (target → smartphone)
- targeted using Symbian OS. (early times)
- & Android & iPhone sys. (recent a)
- MPW can completely disable the phone, delete data, send msgs (Root 2 para pg # 228)

→ Watering-Hole Attacks:- variant of drive-by-downloads attack. The attacker researches their intended victims to identify websites they're likely to visit then scan these sites to identify those w/ vulnerabilities that allow their compromise w/ drive-by-download attack. They then wait for one of their intended victims to visit one of the compromised sites. The attack code may can be written so that it will only infect sys belonging to the target org & take no action against for other visitors to the site. This increases the likelihood of the site compromise remain undetected

Date:

→ Malvertising:- place malware on sites w/o compromising them. Attacker pays for ads for w/ malware incorporated. Malware code may be dynamically generated to infect specific sys to reduce chance of detection. Hard to ~~detect~~ track. Attacker can place these ads for as little as few hours.

→ Clickjacking:- also known as "UI redress attack", vulnerability used by an attacker to collect an infected user's clicks. Can force user to change adjus comp setting, visit website w/ malicious code. Takes adv of Adobe Flash & or JS, attacker can place button under over a legitimate button, making it difficult for user to detect. Tricks user into clicking on a button or link. on a/c page when they were intending to click on top level page. Thus attack is hijacking clicks meant for from one page & routing them to a/c page. Similary keystrokes can also be hijacked. For eg user can be led to believe he/she typing is passed to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Propagation - Social Engineering - Spam, Emails, Trojans

final category of malware → SE (social engineering), i.e tricking users to assist in compromise of their own sys. or personal info.

1- Spam (Unsolicited Bulk) Emails - description of spam (224). Spam email can have an attached doc, which if opened may exploit sfw vulnerability to install malware or it may have attached Trojan horse payload or scripting code that if run can also install malware. Some Trojan can avoid need for user agreement by exploiting sfw vulner. Spam can also be used in phishing attack, typically directing the user to some fake website that mimics some legitimate ~~one~~ service, such as online banking site, where it attempts to capture's user id, password details MIGHTY PAPER PRODUCT or the complete some form w/ sufficient personal details to allow the attacker to impersonate the user in an identity theft.

Date:

ii- Trojan Horse :- useful prog or utility containing hidden code that when invoked performs unwanted or harmful func. TH can be used to accomplish func indirectly. For eg:- entice user to run Trojan prog by incorporating it into a game via a know site dist site or app store.

Three Trojan models :-

1- perform the func of original prog & perform separate malicious activity
2- " " " " " but modify it to perform " "
3- " malicious func that completely replaces the original func

→ share some user features but don't replicate. Eg :- Hydraq Trojan → Operation Aurora 2009 & early 2010. It exploited vulner in Internet Explorer to install itself & targeted several high-profile companies. Dist ming → spam email, watering-hole, fake

→ Call centers & tech support making user install unwanted applications or malware.

3- Mobile Phone Trojans :- first 2004 ; target → smartphone, & Symbian phone earlier
newer targets → android & apple phones.
distributed via apps. Recent eg → phishing Trojans that tricks user into entering banking credential, & ransomware that mimics Google's design style to appear legitimate. (pg# 227)

Date:

Payload – System Corruption

- Once a malware is active, next concern is about its action i.e payload.
- Some malware has nonexistent or non-functional payload - (purpose → spread)
- early payload → destruction on sys when certain trigger cond is met.
- related " → displays unwanted msgs. or content when triggered.
- alo variant inflict real-world damage on the sys.

→ loss of integrity of sys.

- Data Destruction & Ransomware :-
- Chernobyl virus → 1998 seen → Window-95 & 98 viruses. Infected executable files when host is opened. & when trigger date is reached, deletes data. by overwriting 1st megabyte of the hard drive w/ # 0s. resulting in corruption. Occured → 26 April, 1999 & infected 1 million comp.

- Klez mass-mailing worm → Oct 2001 → windows-95 to XP sys. Spreads by emailing copies of itself. to addr found in addr book. on sys. Can stop & del some anti-virus prog. On trigger dates, being 18th of several months each year, empties file.

→ Ransomware :- alternative to destroying data, it encrypts the data. & then demand payments for its recovery. Eg :-
i- PC Cyborg Trojan → 1989
ii- mid-2006 many worms & Trojans appeared → Gpcode Trojan, used public key encryption w/ longer keys.
→ ransom ware spread by via 'drive-by-download' or spam emails.

→ WannaCry ransomware → May 2017. (1st para pg# 228)

Date:

• Real-World Damage :-

→ payloads aims to cause damage to physical equipment. Eg :- Chernobyl virus not only corrupts data but also attempts to rewrite the BIOS code used to initially boot the comp., sys becomes unusable until BIOS chip is reprogrammed or replaced.

→ Recent → Stuxnet worm → control sys. using Siemens industrial control s/w w/ specific config ; then replaces original control w/ to control equipment to operation outside its normal range., resulting in failure of equipment. Target → centrifuge in Iranian uranium enrichment prog.

→ Dec 2015 attack disrupted Ukrainian power sys.

• Logic Bomb :-

→ key comps of data-corrupting malware ; code embedded in malware set to "explode" when certain cond are met. Eg of cond :-

- presence or absence of some files. (eg : pg# 229 1st para)
- particular day, date
- " version or config of sys/s/w
- " user running the app.

→

Payload – Attack Agents: Bots

→ bot, zombie, robot, or drone : secretly takes over a/c Internet attached comp & use it to launch or manage to attacks that are difficult to trace to the bot's creator.

→ compromise system can be :- personal comp, servers, routers, surveillance cameras etc.

→ This type of attack payload's MIGHTY PAPER PRODUCT attacks the integrity & availability of the sys.

Date:

• Botnet :- collection of bots capable of acting in a coordinated manner.

• Uses of Bots :- (pg# 229 – 230)

- Dist DoS attack
- Spamming
- Sniffing traffic
- Keylogging
- Spreading new malware
- Installing adv addons & browser helper objs
- Attacking IRC chat n/w (Internet Relay Chat)
- Manipulating online polls/game

• Remote Control Facility :- RCF distinguishes bot from a worm.

→ worm prop & copy activates itself, whereas bot is controlled by some command-&-control (C&C) server n/w. (can be periodic)

→ early means of implanting RCF used an IRC server.

→ recent " :- comm channel via protocols like HTTP.

→ peer-to-peer protocols to avoid single point of failure.
(pg# 230 – 231)

Payload – Information Theft – Keyloggers, Phishing, Spyware

payloads where the malware gathers data stored on infected sys, attacker can then use it to impersonate the user. These attacks target confidentiality.

• Credential Theft, Keyloggers, & Spyware :-

→ keylogger captures keystrokes to allow an attacker to monitor sensitive info. They implement some filtering mechanism to return info only to a particular site to desired keywords (eg "login" or "password" or "paypal.com").

→ in response to keyloggers, some banking & sites used graphical applet to enter critical info MIGHTY PAPER PRODUCT like pswd. Since the user used text via keyboard. In response attackers developed spyware.

Date:

- spyware monitors wide range of activities, like History, browsing activity, redirecting certain webpage. etc.
  (spware eg.
  → Zeu banking Trojan. → crimeware toolkit ✱

- Phishing & Identity Theft :-
  → capture credential → use URL in spam email. that links to a fake site controlled by the attacker. → phishing.
  → exploits social engineering to leverage users trust by masquerading as comm from trusted source.
  → such spam emails are spread via botnet
  → more dangerous variant is "spear-phishing" attack. This is also an email claiming to be from a trusted source but contain malicious attachments. Recipients are carefully researched by the attacker. & email is carefully crafted to suit its recipient.

- Reconnaissance, Espionage, & Data Exfiltration :-
  (preliminary survey) (spying)
  → reconnaissance payload, which aims to obtain certain types of desired info & return it to the attacker. Eg: Operation Aurora 2009 use Trojan to gain access & then modify source code
  → 2016 Panama Paper leak of millions of doc relating to offshore entities used as tax havens.

Payload - Stealthing - Backdoors, Rootkits
→ hide its presence on sys & provide covert access to that sys. this type of payload also attacks integrity.

Date:

- Backdoor :- also called "trapdoor"; secret entry point into a prog that allows s/o who is aware of backdoor to gain access w/o going through the usual security access procedures.
- Programmers use them to debug & test progs, such backdoor is called "maintenance hook". Used when prog has auth sys that takes a long time. Also used to ensure that there's a method of activating the prog should slt go wrong w/ auth procedure.

→ ~~backdo~~ backdoor is a code that recognizes special sequence of i/p or is triggered by being run from certain userID or event. They become a threat when used to gain unauth access. (para # 3 pg # 233)

→ Backdoor implement as a nlw service, listening on some non-standard port that the attacker can connect to, & issue commands through. Wanacry used backdoor. It ~~Backdoor~~ is difficult to implement in OS. controls for backdoor.

- Rootkit :- set of progs installed on a sys to maintain covert access to that sys. w/ admin (or root) privileges, (hides presence) Rootkit hides by subverting (corrupting) the mechanisms that monitor & report on the procs, files, & registries in comp. A rootkit can be classified into :- (pg # 234)

- persistent	- kernel mode
- memory based	- vm based
- user mode	- external mode

(para below).

Date:

- **Kernel Mode Rootkits:-**
- next generation of rootkits moved down a layer, making changes inside the kernel & co-existing w the OS code inorder to make detection harder.
- primary target of kernel rootkit → system calls, jindex in sys call table
- In Linux, each sys call assigned unique syscall number, which is referred by the procs. Kernel maintain a sys call table, one entry per sys call, routine, contains a pointer to it. 3 tech for to change sys calls:-
  - i - modify sys call table
  - ii - " " " targets } pg#235
  - iii - redirect sys call table

- **VM & Other External Rootkits:-**

latest gen; uses code invisible to the targeted OS; done using regions of compromised VM; rootkit code runs entirely below the visibility of even kernel code. (pg# 236).

Countermeasures

- known as anti-virus; ideal sol → prevention however its nearly impossible.
- ✱ A/c to NIST here are 4 main elements of prevention:-

  policy; awareness; vulnerability mitigation, & threat mitigation.

→ 1st countermeasure should be to ensure all sys are as current as possible inorder to reduce vulnerabilities.

→ 2nd countermeasure → set appl access controls on n/w apps & data stored.

→ 3rd " → user awareness & training.

→ If prevention fails, then 3 technical mechanisms can be used to support following threat mitigation options:- detection; identification; removal

MIGHTY PAPER PRODUCT

Date:

→ if detection succeeds but either identification or removal is not possible then discard infected files & reload a clean backup. ✱

(pg#237)

- **Effective Malware Countermeasures Requirements:-**
  - Generality → handle wide variety of attacks
  - Timeliness → quick response
  - Resiliency → resistance to evasion techs
  - Minimal DOS → should not significantly disrupt normal operations
  - Transparency → countermeasure should not require modification to OS etc
  - Global & Local Coverage.

→ detection may use diff mech that gather data from both host-based and perimeter sensors. (1st para pg# 238)

→ **Host-Based Scanners & Signature-Based Anti-Virus:-**

- first location anti-virus use is on each end sys. which gives it the max access to info.
- anti-virus on personal comp → host-based intrusion detection sys (IDS).
- Advances in virus & anti-virus go hand in hand. 4 gen of anti-virus sftwr:
  - i - 1st generation : simple scanners
  - ii - 2nd " : heuristic "
  - iii - 3rd " : activity traps
  - iv - 4th " : full-featured app protection.

1st gen ⇒ requires malware signature for identification; signature may contain wildcard ent. matches same structure & bit pattern. Limited to detection of known malware. A/c type of 1st gen scanner maintains a record of len of prog & looks for changes in len as a result of a virus infection.

2nd gen ⇒ doesnot rely on specific sign. rather uses heuristic rules: one approach looks for fragments of code often associated w/ malware eg: look beg of enc loop used in polymorphic virus & discover the enc key. then use the key to decrypt & identify the malware, then remove it.

MIGHTY PAPER PRODUCT

Date:

alo approach ⇒ integrity checking ; append checksum to each prog. if its altered / replaced. Then it'll be caught. Or use enc hash func once. key is stored separately from prog so the malware cannot access it. By using a hash func. malware is prevented from producing same hashcode.

3rd gen ⇒ memory resident ; identify malware by actions rather than structure.
- adv → not necessary to develop large sign & heuristics for large set of malware.
- uses dynamic analysis technique.

4th gen ⇒ packages consisting of variety of anti-virus techniques. used in conjunction. like scanning & activity trap components. Also includes access control capability which limits the ability of a malware to penetrate & propa-

→ Sandbox Analysis :-

- one method of detecting & analyzing malware involves running potentially malicious code in an emulated sandbox or a VM. This allows the code to exe in controlled env where its behavior can be closely monitored w/o threatning the security of real sys.
- Running potentially malicious s/w in such env enables detection of complex enc, polymorphic, or metamorphic malware.
- this extended analysis can be used to develop anti-virus signatures of new, unknown malware.

→ difficult design issue w/ sandbox is to determine how long to run each interpretation. Typical malware activates as soon after a program exe, but recent malware uses evasion such as extended sleep to evade detection. in the analysis time used by sandbox sys. Sandbox analysis has only limited amount of time. & resources available

(1st para pg# 240)

Date:

- Host-Based Dynamic Malware Analysis :-

- dynamic malware analysis or behavior-blocking s/w integrates w/ the OS of a host comp & monitors prog behavior in real time for malicious actions.
- It is type of host-based intrusion prevention sys, s/w monitors behavior of possibly malicious code & has the capability to block malicious actions before any affect. Monitored behavior can include :-
  - → attempt to open, view, delete, and/or modify files.
  - → " " format disk drives & other unrecoverable disk operations.
  - → Modification to the logic of executable files or macros
  - → " of critical sys settings, such as start-up settings.
  - → Scripting of email & instant msging clients to send executable content.
  - → Initiation " n/w. comm.

Limitation ⇒ b/c malicious code must run on the target m/c before all its behavior can be identified, it can cause harm before it has been detected & blocked.

- Spyware Detection & Removal :- pg# 240
- Rootkit Countermeasures :- pg# 241.

- Perimeter Scanning Approaches :-

anti-virus is used on servers, firewall and IDS. Typically included in email, web proxy services. May also be included in traffic analysis component of an IDS. provides larger scale view of malware activity. May also include intrusion prevention measures, blocking flow of any suspicious traffic thus preventing it reaching & compromising some target sys. However this approach is limited to scanning malware content, no access to any behavior observed on an infected sys.

Date: _____

→ 2 types of monitoring s/w may be:-

1) Ingress Monitors:- located at border b/w the enterprise n/w & the Internet. can use either anomally or signature & heuristics approaches to detect malware. A honeypot can also capture incoming malware traffic. Eg:- look for incoming traffic to unused local IP addr.

2) Egress Monitors:- located at egress (exit) point on individual LANs on the enterprise n/w as well as border b/w enterprise n/w & Internet. It is designed to catch the source of a malware attack by monitoring outgoing traffic. Could look for common sequential or random scanning behaviour used by worms & rate limit or block it. May also be able to detect & respond to abnormally high email traffic. May also implement data exfiltration "data-loss" countermeasures.

→ Perimeter monitoring can also assist in detecting & responding to botnet activity. by detecting abnormal traffic ~~bot~~ patterns. Primary objective is to detect & ~~destroy~~ disable the botnet during its construction phase.

(pg # 242)