

# EVENTS AND INCIDENT

# WHAT IS AN EVENT

- An event is any observable occurrence in a system or network.
- Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.
- Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.
- As far as our field is concerned, We will only address adverse events that are computer security related, not those caused by natural disaster or power failures.

# WHAT IS COMPUTER SECURITY INCIDENT

- A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents are:
  - An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
  - Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
  - An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
  - A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

## CONT.

- In the context of information technology, an incident is an event that disrupts operational processes.
- An incident may involve the failure of a feature or service that should have been delivered or some other type of operation failure.
- Security incidents are events that indicate that an organization's systems or data may have been compromised.

## CONT.

- It is an act of violating explicit or implied security policy resulting in, unauthorized access, denial of service/disruption, and unauthorized use of a system for processing or storage of data or change to system software, hardware, firmware characteristics without the owner's knowledge.
- Incidents include minor disruptions, such as running out of disk space on a desktop machine, as well as major disruptions, such as data breaches involving the exposure of sensitive information.

CONT.

- Each organization must define what a computer security incident is for their site.
- Examples of general definitions for a computer security incident could be:
  - “Any real or suspected adverse event in relation to the security of computer systems of computer networks”
  - “The act of violating an explicit or implied security policy”

## TYPES OF INCIDENTS

- DoS and DDoS
- MiTM attack
- Phishing or Pharming attack
- Drive-by attack
- Password attack
- SQL Injection
- Eavesdropping attack
- Malware attack
- Vulnerability Scanning

# TYPES OF MALWARE

- Viruses
- Spyware
- Adware
- Ransomware
- Keylogger
- Botnet
- Backdoor
- Downloader
- Launcher
- Rootkit
- Scareware
- Spamware



# VIRUSES

- Created to relentlessly self-replicate it infects programs and files. The malicious activities may be targeted at destroying valuable data or causing unrepairable damages

# BACKDOOR

- Malicious code that installs itself onto a computer to allow the attacker access.
- Backdoors usually let the attacker connect to the computer with little or no authentication and execute commands on the local system.

# DOWNLOADER

- Malicious code that exists only to download other malicious code.
- Downloaders are commonly installed by attackers when they first gain access to a system.
- The downloader program will download and install additional malicious code.

# LAUNCHER

- Malicious program used to launch other malicious programs.
- Usually, launchers use nontraditional techniques to launch other malicious programs in order to ensure stealth or greater access to a system.

# ROOTKIT

- Malicious code designed to conceal the existence of other code.
- Rootkits are usually paired with other malware, such as a backdoor, to allow remote access to the attacker and make the code difficult for the victim to detect.

# SPYWARE

- The software is created to spy on the victim.
- It is secretly implanted on the computing device by the hacker.
- The spyware gathers information and sends it to the hacker.

# ADWARE

- The malicious program is devised to pop-up unwanted advertisements on the victim's computer without their permission.
- The pop-ups are uncontrollable and tend to behave erratically.

# SCAREWARE

- Malware designed to frighten an infected user into buying something.
- It usually has a user interface that makes it look like an antivirus or other security program.
- It informs users that there is malicious code on their system and that the only way to get rid of it is to buy their “software,” when in reality, the software it’s selling does nothing more than remove the scareware.



# SPAMWARE

- Malware that infects a user's machine and then uses that machine to send spam.
- This malware generates income for attackers by allowing them to sell spam-sending services.

# RANSOMWARE

- The ransom malware blocks the user from accessing the files or programs and the malware removal demands to pay the ransom through certain online payment methods.
- Once the amount is paid the user can resume using their system.

## KEY-LOGGER

- Tools designed to record every keystroke on the affected machine for later retrieval
- It stores the data regarding each and every key user presses on the keyboard.
- It is very commonly used method to get username and passwords from a legitimate user.

# BOTNET

- The cybercriminal blocks a user actions and takes full control of the system.
- The hacker creates a network of malware-infected computers which functions as a bot.
- The botnet is used to transmit malware, send spam emails, and execute other malicious tasks.

**SIGN OF AN INCIDENT**

## SIGN OF AN INCIDENT

- Signs of an incident fall into one of two categories: precursors and indicators.
  - A precursor is a sign that an incident may occur in the future.
  - An indicator is a sign that an incident may have occurred or may be occurring now.

## SIGN OF AN INCIDENT

- Most attacks do not have any identifiable or detectable precursors from the target's perspective.
- If precursors are detected, the organization may have an opportunity to prevent the incident by altering its security posture to save a target from attack.

## SIGN OF AN INCIDENT

- Examples of precursors are:
  - Web server log entries that show the usage of a vulnerability scanner.
  - An announcement of a new exploit that targets a vulnerability of the organization's mail server.
  - A threat from a group stating that the group will attack the organization.



# SIGN OF AN INCIDENT

- While precursors are relatively rare, indicators are all too common.
- Too many types of indicators exist to exhaustively list them, but some examples are listed below:
  - A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server.
  - Antivirus software alerts when it detects that a host is infected with malware.
  - A system administrator sees a filename with unusual characters.
  - A host records an auditing configuration change in its log.
  - An application logs multiple failed login attempts from an unfamiliar remote system.
  - An email administrator sees a large number of bounced emails with suspicious content.
  - A network administrator notices an unusual deviation from typical network traffic flows.

# INCIDENT CATEGORY

- Generally, Incidents are divided into three main categories:
  - High
  - Medium
  - Low

## INCIDENT CATEGORY - HIGH

- The severity of a security incident will be considered “high” if any of the following conditions exist:
  - Threatens to have a significant adverse impact on a large number of systems and/or people (for example, the entire UNIT is affected)
  - Poses a potential large financial risk or legal liability to the Organization.
  - Threatens confidential data (for example, the compromise of a server that contains or names with social security numbers or credit card information)

## INCIDENT CATEGORY - HIGH

- It adversely impacts an enterprise system or service critical to the operation of a major portion of the organization (for example, e-mail, customer information system, Financial information system, human resources information system, etc.).
- It poses a significant and immediate threat to human safety, such as a death-threat to an individual or group.
- It has Has a high probability of propagating to many other systems on premise and/or off premise and causing significant damage or disruption.
- High severity incidents require an immediate response and focused, dedicated attention by the CISO and other appropriate officials and IT security staff until resolved.

## INCIDENT CATEGORY - MEDIUM

- The severity of a security incident will be considered “medium” if any of the following conditions exist:
  - Adversely impacts a moderate number of systems and/or people, such as an individual department, unit, or building
  - Adversely impacts a non-critical enterprise system or service
  - Adversely impacts a departmental system or service, such as a departmental file server
  - Disrupts a building or departmental network
  - Has a moderate probability of propagating to other systems on premise and/or off premise and causing moderate damage or disruption

## INCIDENT CATEGORY - MEDIUM

- Medium severity incidents require a quick response by appropriate personnel (usually from the affected unit) who have primary responsibility for handling the incident.

## INCIDENT CATEGORY - LOW

- Low severity incidents have the following characteristics:
  - Adversely impacts a very small number of systems or individuals
  - Disrupts a very small number of network devices or segments
  - Has little or no risk of propagation or causes only minimal disruption or damage in their attempt to propagate
- Since a single compromised system can “wake up” and negatively affect other systems at any time, appropriate personnel (usually the technical support staff responsible for the system) must respond as quickly as possible, no later than the next business day.

# IDENTIFY AN INCIDENT

- Event Management
  - Event Management provides qualified alerts when one or more Configuration Items (CI) have have encountered a disruption in its normal functioning or may encounter disruption in its normal functioning. In practice, Event Management may lead to generation of a manual incident OR an automated incident creation.
- From Web Interface
  - Web interface is a very efficient method to identify incidents as it involves no human interface to log the ticket. Organization need to provide a intuitive interface to the end users to log incidents.



## IDENTIFY AN INCIDENT

- Phone Calls
  - Phone calls is the most common way of reporting incidents. This is a labor intensive method to report incidents. However this method has its own merits as end-user incidents can be quickly resolved via First Call Resolution, thus improving customer satisfaction substantially.
- Email Interface
  - Emailing incident details to Service Desk is the easiest method to report an incident. However, in most cases, this mode of incident reporting is rigged with lot of inefficiencies.