Sharing Is Caring. If you enjoy this article, help us share with others.

Digital Forensics In Cybersecurity: Facts To Note

Now that you have investigated and identified valid alerts, what do you do with the evidence? The cybersecurity analyst will inevitably uncover evidence of criminal activity. In order to protect the organization and to prevent cybercrime, it is necessary to identify threat actors, report them to the appropriate authorities, and provide evidence to support prosecution.

Tier 1 cybersecurity analysts are often the first to uncover wrongdoing. Cybersecurity analysts must know how to properly handle evidence and attribute it to threat actors. In this article, we will be talking about some of the facts that you need to know about Digital Forensics in cybersecurity.

Digital forensics is the recovery and investigation of information found on digital devices as it relates to criminal activity. Indicators of compromise are the evidence that a cybersecurity incident has occurred.

This information could be data on storage devices, in volatile computer memory, or the traces of cybercrime that are preserved in network data, such as pcaps and logs. It is essential that all indicators of compromise be preserved for future analysis and attack attribution.

Cybercriminal activity can be broadly characterized as originating from inside of or outside of the organization. Private investigations are concerned with individuals inside the organization.

These individuals could simply be behaving in ways that violate user agreements or other non-criminal conduct. When individuals are suspected of involvement in criminal activity involving the theft or destruction of intellectual property, an organization may choose to involve law enforcement authorities, in which case the investigation becomes public.

Internal users could also have used the organization’s network to conduct other criminal activities that are unrelated to the organizational mission but are in violation of various legal statutes.

In this case, public officials will carry out the investigation.

When an external attacker has exploited a network and stolen or altered data, evidence needs to be gathered to document the scope of the exploit. Various regulatory bodies specify a range of actions that an organization must take when various types of data have been compromised. The results of forensic investigation can help to identify the actions that need to be taken.

For example, under the US HIPAA regulations, if a data breach has occurred that involves patient information, notification of the breach must be made to the affected individuals. If the breach involves more than 500 individuals in a state or jurisdiction, the media, as well as the affected individuals, must be notified.

A digital forensic investigation must be used to determine which individuals were affected, and to certify the number of affected individuals so that appropriate notification can be made in compliance with HIPAA regulations.

It is possible that the organization itself could be the subject of an investigation. Cybersecurity analysts may find themselves in direct contact with digital forensic evidence that details the conduct of members of the organization.

Analysts must know the requirements regarding the preservation and handling of such evidence. Failure to do so could result in criminal penalties for the organization and even the cybersecurity analyst if the intention to destroy evidence is established.

The Digital Forensics Process

It is important that an organization develop well-documented processes and procedures for digital forensic analysis. Regulatory compliance may require this documentation, and this documentation may be inspected by authorities in the event of a public investigation.
NIST Special Publication 800-86 *Guide to Integrating Forensic Techniques into Incident Response* is a valuable resource for organizations that require guidance in developing digital forensics plans.For example, it recommends that forensics be performed using the four-phase process.
The following describes the four basic phases of the digital evidence forensic process.
This image depicts the Digital Evidence Forensic Process in a progress bar moving from right to left.
The four steps are Collection, Examination, Analysis, and Reporting. Above the steps are listed the inputs or outputs for each step. Media is collected, and the examination results in data, Analysis yields information, and evidence is reported.

The Digital Evidence Forensic Process

Types of Evidence

In legal proceedings, evidence is broadly classified as either direct or indirect. Direct evidence is evidence that was indisputably in the possession of the accused or is eyewitness evidence from someone who directly observed criminal behaviour.
Evidence is further classified as:

- **Best evidence** – This is evidence that is in its original state. This evidence could be storage devices used by an accused, or archives of files that can be proven to be unaltered.
- **Corroborating evidence** – This is evidence that supports an assertion that is developed from the best evidence.
- **Indirect evidence** – This is evidence that, in combination with other facts, establishes a hypothesis. This is also known as circumstantial evidence. For example, evidence that an individual has committed similar crimes can support the assertion that the person committed the crime of which they are accused.

Evidence Collection Order

IETF RFC 3227 provides guidelines for the collection of digital evidence. It describes an order for the collection of digital evidence based on the volatility of the data. Data stored in RAM is the most volatile, and it will be lost when the device is turned off. In addition, important data in volatile memory could be overwritten by routine machine processes.
Therefore, the collection of digital evidence should begin with the most volatile evidence and proceed to the least volatile, as shown in the figure.
This image uses a downward-pointing arrow, graded in color from red to green, to assign a level of volatility to certain evidence sources.
The most volatile source listed is the contents of RAM, the source with mid-level volatility is listed as the contents of fixed disks, and the source that is listed as non-volatile is archived backup data.

Evidence Collection Priority

Evidence
SourceContents of Fixed DisksNon-volatileVolatileContents of RAMArchived Backup Data

An example of most volatile to least volatile evidence collection order is as follows:

1. Memory registers, caches
2. The routing table, ARP cache, process table, kernel statistics, RAM
3. Temporary file systems
4. Non-volatile media, fixed and removable
5. Remote logging and monitoring data
6. Physical interconnections and topologies
7. Archival media, tape or other backups

Details of the systems from which the evidence was collected, including who has access to those systems and at what level of permissions should be recorded. Such details should include hardware and software configurations for the systems from which the data was obtained.

Chain of Custody

Although evidence may have been gathered from sources that support attribution to an accused individual, it can be argued that the evidence could have been altered or fabricated after it was collected. In order to counter this argument, a rigorous chain of custody must be defined and followed.

Chain of custody involves the collection, handling, and secure storage of evidence. Detailed records should be kept of the following:

- Who discovered and collected the evidence?
- All details about the handling of evidence including times, places, and personnel involved.
- Who has primary responsibility for the evidence, when responsibility was assigned, and when custody changed?
- Who has physical access to the evidence while it was stored? Access should be restricted to only the most essential personnel.

Data Integrity and Preservation

When collecting data, it is important that it is preserved in its original condition. Timestamping of files should be preserved. For this reason, the original evidence should be copied, and analysis should only be conducted on copies of the original. This is to avoid accidental loss or alteration of the evidence. Because timestamps may be part of the evidence, opening files from the original media should be avoided.

The process used to create copies of the evidence that is used in the investigation should be recorded. Whenever possible, the copies should be direct bit-level copies of the original storage volumes.

It should be possible to compare the archived disc image and the investigated disk image to identify whether the contents of the investigated disk have been tampered with. For this reason, it is important to archive and protect the original disk to keep it in its original, untampered with, condition.

Volatile memory could contain forensic evidence, so special tools should be used to preserve that evidence before the device is shut down and evidence is lost. Users should not disconnect, unplug, or turn off infected machines unless explicitly told to do so by security personnel.

Following these processes will ensure that any evidence of wrongdoing will be preserved, and any indicators of compromise can be identified.

Attack Attribution

After the extent of the cyberattack has been assessed and evidence collected and preserved, incident response can move to identify the source of the attack. As we know, a wide range of threat actors exist, ranging from disgruntled individuals, hackers, cybercriminals and criminal gangs, or nation-states.

Some criminals act from inside the network, while others can be on the other side of the world. The sophistication of cybercrime varies as well. Nation-states may employ large groups of highly-trained individuals to carry out an attack and hide their tracks, while other threat actors may openly brag about their criminal activities.

Threat attribution refers to the act of determining the individual, organization, or nation responsible for a successful intrusion or attack incident.Identifying responsible threat actors should occur through the principled and systematic investigation of the evidence.

While it may be useful to also speculate as to the identity of threat actors by identifying potential motivations for an incident, it is important not to let this bias the investigation. For example, attributing an attack to a commercial competitor may lead the investigation away from the possibility that a criminal gang or nation-state was responsible.

In an evidence-based investigation, the incident response team correlates Tactics, Techniques, and Procedures (TTP) that were used in the incident with other known exploits. Cybercriminals, much like other criminals, have specific traits that are common to most of their crimes.

Threat intelligence sources can help to map the TTP identified by an investigation to known sources of similar attacks. However, this highlights a problem with threat attribution. Evidence of cybercrime is seldom direct evidence. Identifying commonalities between TTPs for known and unknown threat actors is circumstantial evidence.

Some aspects of a threat that can aid in attribution are the location of originating hosts or domains, features of the code used in malware, the tools used, and other techniques. Sometimes, at the national security level, threats cannot be openly attributed because doing so would expose methods and capabilities that need to be protected.

For internal threats, asset management plays a major role. Uncovering the devices from which an attack was launched can lead directly to the threat actor. IP addresses, MAC addresses, and DHCP logs can help track the addresses used in the attack back to a specific device. AAA logs are very useful in this regard, as they track who accessed what network resources at what time.

The MITRE ATTACK Framework

One way to attribute an attack is to model threat actor behavior. The MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) Framework enables the ability to detect attacker tactics, techniques, and procedures (TTP) as part of threat defence and attack attribution.

PEOPLE ALSO READ: Cyber Killer Chain In Cybersecurity: Facts To Know
Powered by **Inline Related Posts**

This is done by mapping the steps in an attack to a matrix of generalized tactics and describing the techniques that are used in each tactic. Tactics consist of the technical goals that an attacker must accomplish in order to execute an attack and techniques are the means by which the tactics are accomplished.

Finally, procedures are the specific actions taken by threat actors in the techniques that have been identified. Procedures are the documented real-world use of techniques by threat actors.

The MITRE ATT&CK Framework is a global knowledge base of threat actor behaviour. It is based on observation and analysis of real-world exploits with the purpose of describing the behaviour of the attacker, not the attack itself. It is designed to enable automated information sharing by defining data structures for the exchange of information between its community of users and MITRE.

The figure shows an analysis of ransomware exploits from the excellent ANY.RUN online sandbox. The columns show the enterprise attack matrix tactics, with the techniques that are used by the malware arranged under the columns. Clicking the technique then lists details of the procedures that are used by the specific malware instance with a definition, explanation, and examples of the technique.

Note: Do an internet search on MITRE ATT&CK to learn more about the tool.

MITRE ATT&CK Matrix for a Ransomware Exploit

Action Point

https://spoo.me/iy8taz

P.S.: If you need private online training on any of the ICT courses I offer here and you are in Nigeria, please send me a DM on my WhatsApp at **+2348103180831.** Please note that the Training will be 100percent online. It will be delivered via Zoom or Google Meet.

PS: I know you might agree with some of the points raised in this article or disagree with some of the issues raised.

Please share your thoughts on the topic discussed. We would appreciate it if you could drop your comment. Thanks in anticipation.

Sharing Is Caring. If you enjoy this article, help us share with others.

Related posts:

1. The 10x Son. The Making of an Extraordinary Chap
2. The 10x Whatsapp Group Administrator . Being a Leader With a Difference
3. The 10x Employee. Building Leaders in Our Organisations
4. Building a 10x Career. The Untaken Path to Career Growth