Attribution and its Limitations

Attribution is the determination of a cause or origin of an action. In the realms of cybersecurity, we are primarily concerned about this when malicious actors are in play, and determining who, what or where a cyber breach or intrusion has occurred. Attribution is not solely focused on laying blame but gathering information, a new user may inadvertently cause a system failure, this would be attributed to inexperience rather than a malicious act.

Machine Attribution

Attributing malicious cyber activity to a machine or multiple machines would mean identifying the machine(s) used in an attack. This would usually require examining things like the IP address, log files that document what is happening in the network, who has logged in to the machine. So, we could find out that Azleon's machine was used in an attack but find a trail leading to Jupiter's machine which was the originating point of attack. There could be multiple machines in a trail. The IP address may be in another country or require further investigation. Should the IP lead back to Azleon then law enforcement could seize that machine for investigation.

Human Attribution

Attributing the malicious activity to a human is finding the identity of the person(s) responsible for the activity, those pushing the keys as it were. Technical forensics which look at data left behind may not be able to help much further, credentials may point to one person but that may not have been the person physically executing the attack. Credentials get stolen or machine compromised. Technical means may not be enough to identify the person involved as data collected would need to be compared to a database to match an identity, therefore it is only as good as the database. If you can identify the person responsible it is vital to know why it was carried out and if other parties were involved.

Ultimately Responsible Attribution

Attributing this malicious activity to the ultimately responsible party answers the questions of: Who is to blame? Was the actor working alone and fully responsible or working on behalf of an organization or nation state? The "why" is often a more important factor here as people can be coerced into committing these acts, or may be in a position that they feel they can't refuse. Law enforcement could decide to prosecute an individual or a nation could decide to engage in diplomatic discussion with the offending nation, they might then attribute this to an organization and prosecute or even retaliate.

As you can see the process of assigning attribution can be difficult and complicated, even more so when it is easy to use proxies in other countries. Then requiring deeper and longer investigations will need more cooperation with other agencies.

Key Indicators to attribution

- **Tradecraft** – Frequently used behaviors such as an attacker's techniques, tools and procedures used to conduct cyber-attack.

- **Infrastructure** – The physical machines or networks used in the attack; these are often compromised by other means before an attack.
- **Malware** – Malware can be specific to a threat actor; it can be reused or it can be modified quickly if a compromise is suspected to avoid attribution.
- **Intent** – The intent behind the attack, the motivation or reasoning.
- **External sources** – External reports from organizations like cyber security companies, media even students

Cyber Attribution Techniques

Investigators use many different tools and programs to reveal information about attacks. Take a piece of malware if this was written in non-native language such as one using the Cyrillic alphabet, this information can be used for cyber attrition.

Cyber attackers often want notoriety for their work and may use certain flairs of style or distinctive techniques that can be recognized and used to identify them. They may use a particular social engineering technique or have written their own malware and repeatedly used it.

Issues with Attribution

A major difficulty in analyzing data from attacks is to determine what can be reliable. Metadata such as source IP addresses, email data, domain names, user names, and registration data can all be helpful. Still, it may be faked, through proxies and by using other compromised targets to carry out the attack. The Tor browser can enhance anonymity for malicious actors and automatically encrypts traffic.

Threat actors may choose to share infrastructure to make attribution to a single group harder, or use commodity malware or living-off-the-land techniques to prevent identification via the use of unique tools or techniques. Copy-cat attacks can occur where one malicious actor will use the same tools and techniques as another actor in an attempt to trick researchers and threat intelligence analysts into believing the attack was conducted by the other group.

Previous Topic | Mark Complete | Next Topic
Back to Lesson