Cyber threat intelligence

Intelligence is defined as information gathered either by human means (Human Intelligence or HUMINT) or by electronic means (Signal Intelligence or SIGINT) combined with a cognitive process that adds value. This information with its added value is called intelligence. Intelligence is used to make decisions in political and economic life, and even more so in a military context. Cyberspace is no exception to the fact that intelligence is vital for both the attacker and the (potential) victim.

A cyber threat is defined as a danger that can compromise the security, integrity or confidentiality of computer systems, networks, data or users. There are several types: ransomware, denial-of-service attacks designed to saturate a site's servers and crash the site in question, social engineering, etc. There are many reasons for an attack: the lure of gain generally, revenge, exploitation (sometimes in the mistaken belief that penetrating a network without authorisation will lead to a job), espionage, destabilisation, strategic pre-positioning. The profiles are also diverse: it can be the employee of an organisation without much computer knowledge (especially at a time when hacking "kits" can be bought on the dark web), more or less experienced and organised cybercriminals, a teenager "having fun" or the top of the food chain: the Advanced Permanent Threats, which are criminal groups more or less supported by States (Russia, North Korea, Iran, etc.).

The stakes are enormous. Sad as it is, we are only as good as our data. So our data, including our personal data, is worth its weight in gold. That's why some people want to get their hands on it. Any attack requires a minimum of preparation, and every preparation makes a "noise". And it's this noise that needs to be collected, analysed and analysed to derive intelligence, which can then be passed on to the originator and finally (ideally) reported back to them... so that we can start again. This process is called the intelligence process.

While business intelligence is (relatively) better known than cyber threat intelligence, and therefore the sources are better known, the question arises as to how (anyone) can conduct cyber threat intelligence to protect the organisation to which they belong.

I Analysis of a cyber attack

Robert Aaron, one of the UK's leading authorities on cyber threat intelligence, has drawn up a model. While this model does not claim to be exhaustive in terms of the parameters to be taken into account, it does provide a good basis for any analyst wishing to analyse an attack. This model is that of the diamond, where we analyse :

- The identity of the opponent: who is she? Why is she doing it? What is the initial point of entry into the network (IP address/email address)? Attributing the attack to a specific actor remains horribly difficult...
- The victim's identity: who is she? Does the victim support controversial political or social positions? Is the victim labelled, rightly or wrongly, as "pro-Y" or "anti-X"? Does the victim have available cash? Is the victim who clicked on the link included in the violated databases? Is their access protected? Does the victim need to be made aware of security issues to ensure that this does not happen again?
- Infrastructure: this involves researching the infrastructure used. For once, this will be determined using the famous "Who? Who? When? When? What? Why? How much? how the infrastructure used was contaminated/affected.
- Capabilities: finally, it is necessary (although very difficult) to identify the approach used by the opponent. How was he able to exploit the victim? Here, we need to start from hypotheses based on the previous questions in the model and validate them.

These questions are by no means exhaustive. Depending on the case, other questions will be raised.
But they do help us to understand how the cyber attack came about.

II the MITRE ATT&CK framework

If you want to gather intelligence, you need to use sources that can provide knowledge or insights to help you understand the attackers and anticipate their actions.

This is also true when it comes to intelligence on cyber threats. The first source to exploit is the MITRE ATT&CK framework[1] .
It stands for "Adversarial Tactics, Techniques and Common Knowledgell". In practical terms, it is a tool that can be used to improve IT security by providing a database of the tactics and techniques used by cybercriminals throughout the attack lifecycle. The information comes from a community of watchdogs, public incident reports, and research into new techniques by cybersecurity analysts and threat hunters. The MITRE ATT&CK framework lists 14 tactics:

- Recognition
- Development of resources
- Initial access
- Execution
- Persistence
- Elevation of privileges
- Bypassing defences
- Access to identifiers
- Discover
- Lateral displacement
- Collection
- Command and control
- Exfiltration
- Impact

Why is this base so important? Because human behaviour does not change. If the technical tools evolve, it is important to understand that human behaviour does not change. If human behaviour does not change, the methodology will not change. So, in any attack, there are these phases, although in reality there are more:

- **Reconnaissance**: the attacker will also gather intelligence on his target.
- **Armament**: the attacker will prepare his "exploit", which he will use on his target.

[1] https://attack.mitre.org

- **Delivery**: the attacker will deliver his "exploit" to his target either by email, USB key or the web. This is where social engineering comes in. For example, if the research on the target has determined that the person has been single for a long time, an exploit will have to be prepared to make the target want to click on a link (dating, for example). Here, psychological levers such as MICE (Monney, Interest, Constraint, Ego) or its French equivalent SANSOUCIS (Solitude, Argent, Nouveauté, Sexe, Orgueil, Utilité, Contrainte, Idéologie, Suffisance) will be used.
- **Exploitation**: once the payload has been delivered, the attacker exploits the vulnerabilities (identified during the reconnaissance phase) to execute the target's code.
- **Installation**: the attacker can install other software in order to attack other systems or ensure that the payload persists on the victim's network.
- **Command and control (C2)**: the attacker will set up a channel to remotely control the target's system.
- **Actions on objectives**: this is the last stage where the attacker achieves his initial objectives: exfiltration of data, execution of the software ransom or any other action.

Given the terrible financial damage caused by cyber attacks (€2 billion in France by 2022, not counting the sociological and psychological effects), there will come a day when insurance companies will no longer want to insure against cyber risks... insurance companies themselves are beginning to be attacked[2] . French companies would be well advised to look into the problem and recruit analysts to anticipate cyber attacks.

L'article est unique et a été rédigé par un bénévole expert de chez ADESS, ayant une grande expertise dans sa thématique de prédilection. Il a accumulé une expérience professionnelle significative et des diplômes qui lui sont associés.

ADESS n'a aucune intention d'approuver ou d'infirmer les opinions exprimées dans les publications, qui restent la propriété de leurs auteurs :

Pierre VERDIN – ID : 7319745

[2] https://www.newsassurancespro.com/sante-un-deuxieme-operateur-de-tiers-payant-victime-de-cyber-attaque/01691586519

Source de l’article sur : www.adess-france.fr