Cyber Threat Intelligence (CTI)

### **What is threat intelligence?**

Threat intelligence, also known as cyber threat intelligence (CTI), is information gathered from a range of sources about current or potential attacks against an organization. The information is analyzed, refined and organized and then used to minimize and mitigate cybersecurity risks.

The main purpose of threat intelligence is to show organizations the various risks they face from external threats, such as [zero-day](https://www.techtarget.com/searchsecurity/definition/zero-day-vulnerability) threats and advanced persistent threats ([APTs](https://www.techtarget.com/searchsecurity/definition/advanced-persistent-threat-APT)). Threat intelligence includes in-depth information and context about specific threats, such as who is attacking, their capabilities and motivation, and the indicators of compromise ([IOCs](https://www.techtarget.com/searchsecurity/definition/Indicators-of-Compromise-IOC)). With this information, organizations can make informed decisions about how to defend against the most damaging attacks.

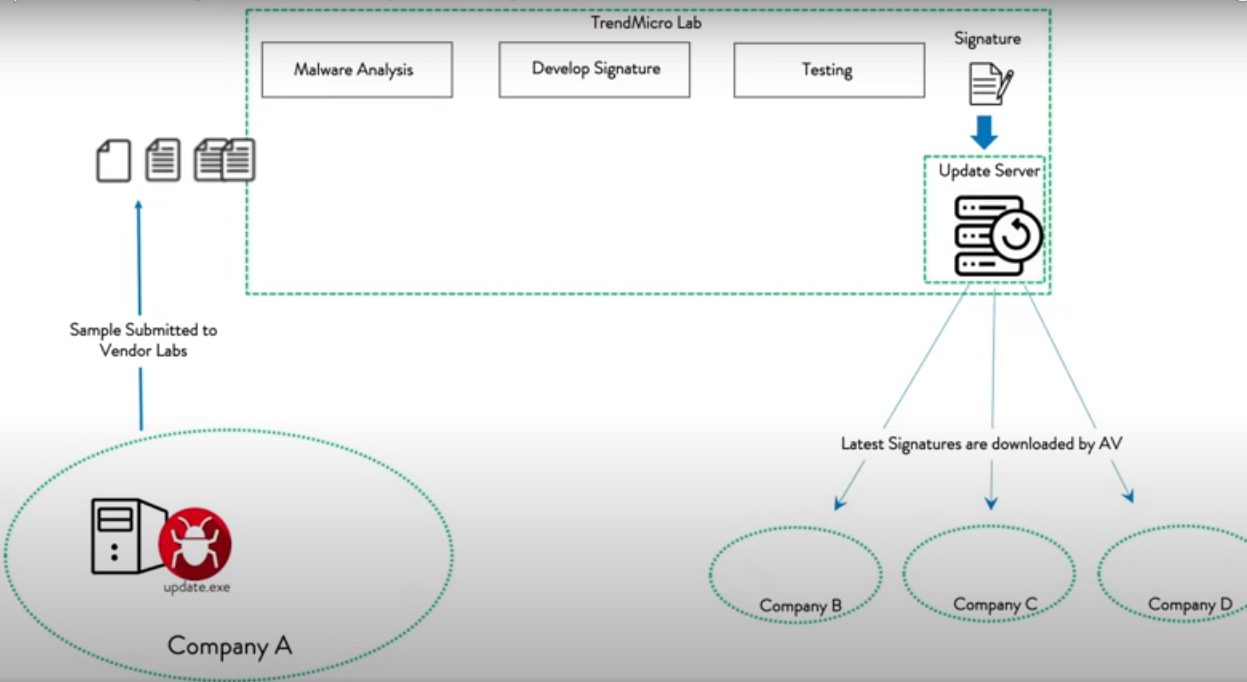
### **Why is threat intelligence important?**

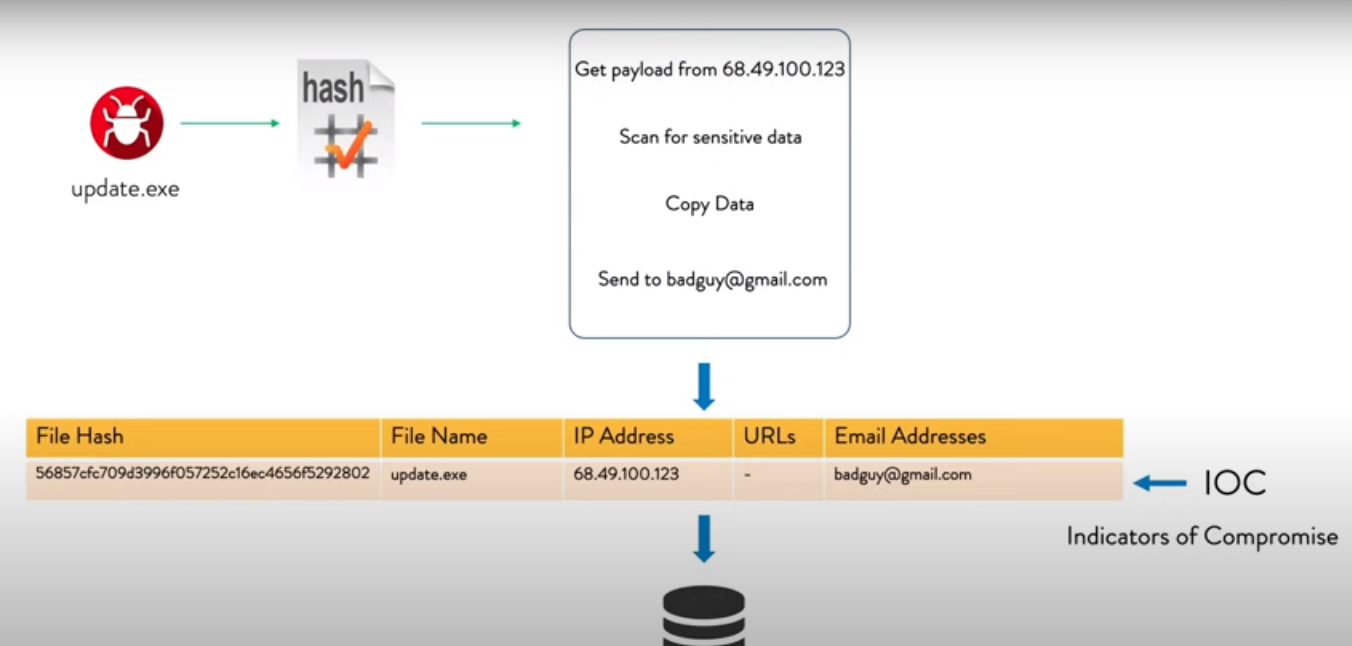
In a military, business or security context, intelligence is information that provides an organization with decision support and possibly a strategic advantage. Threat intelligence is a part of a bigger [security intelligence](https://www.techtarget.com/whatis/definition/security-intelligence-SI) strategy. It includes information related to protecting an organization from external and inside threats, as well as the processes, policies and tools used to gather and analyze that information.

Threat intelligence provides better insight into the threat landscape and threat actors, along with their latest tactics, techniques and procedures. It enables organizations to be proactive in configuring its security controls to detect and prevent advanced attacks and zero-day threats. Many of these adjustments can be automated so security stays aligned with the latest intelligence in real time.

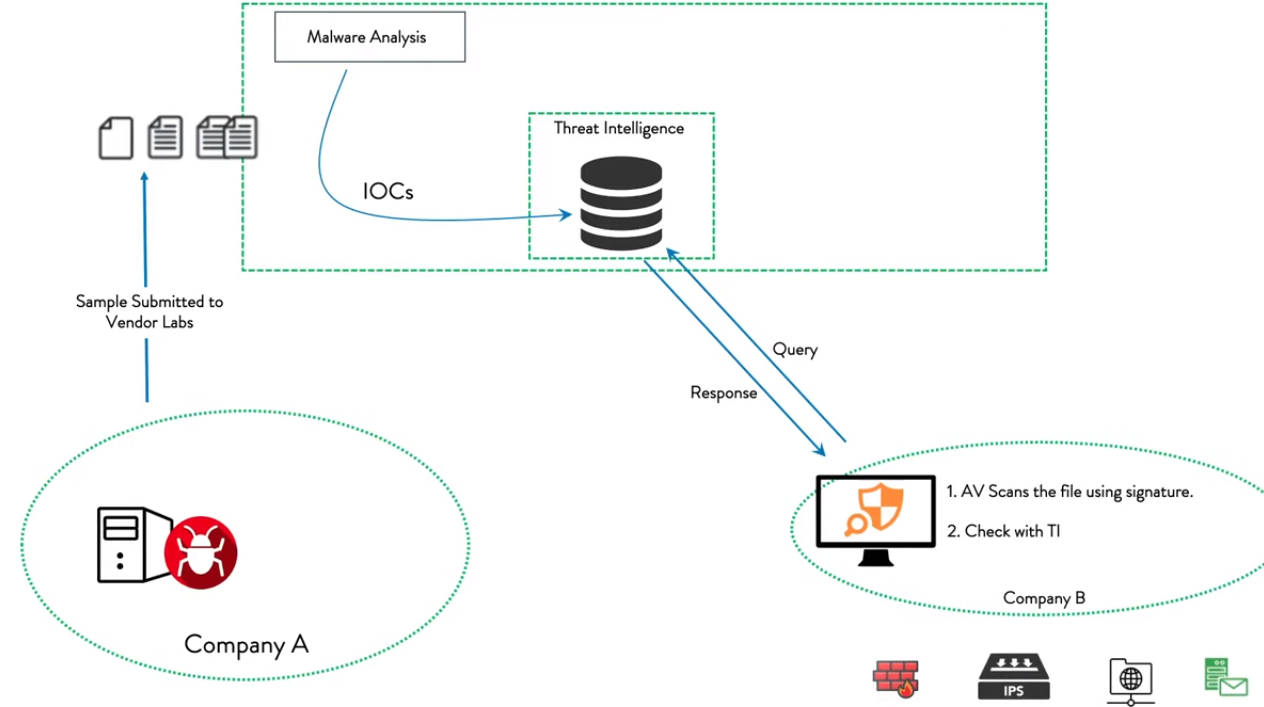
**Example of Threat Intelligence:**

before threat intelligence. The identification and sharing of new malware takes many months to be delived to end points





**with the collected IOC for the threat, it became easier to share information of the malware and the end points can detect new threat using the IOC and take actions**



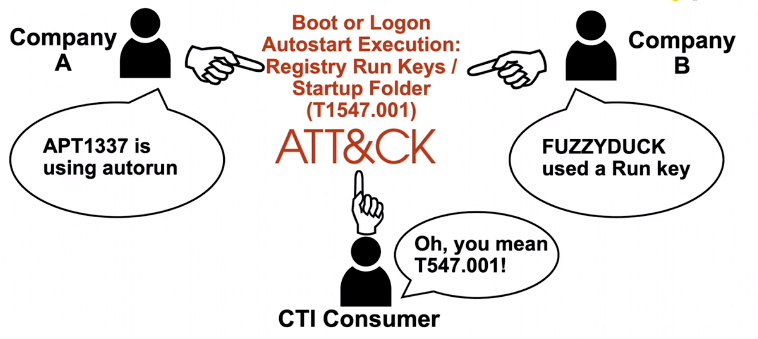
**with the sharing of threat intelligence it is easy to identify zero day threat.**

**How CTI helps defender and community?**

CTI provide information related to attack by spcific or group of APT, defender can check if such technique can be detected or not and take required actions to handle it.



When the CTI do the analysis and share the information in common way, i.e mapping it to ATT&CK, then it becomes easy for CTI consumer.

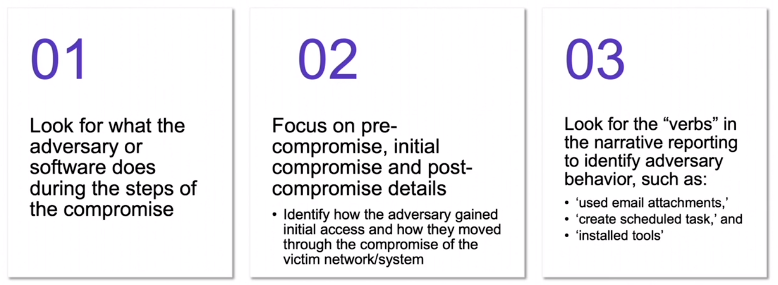


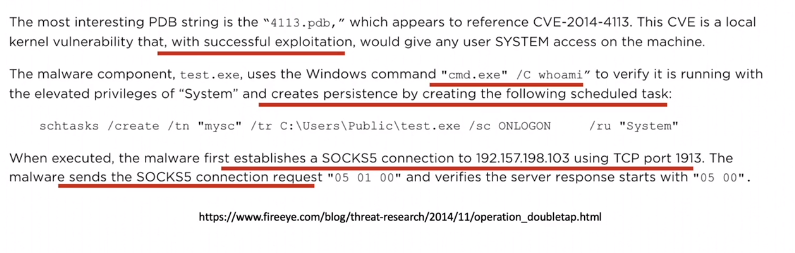
**ATT&CK Mapping Process:**



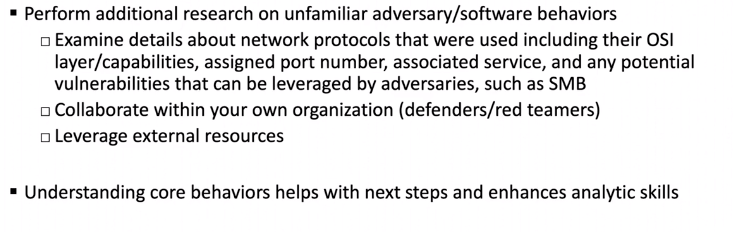
**1) Finding and researching the behaviour:**

Step 1: Finding behaviour:

sample behaviour: highlighted are some adversary behaviour



Step2: research the behaviour



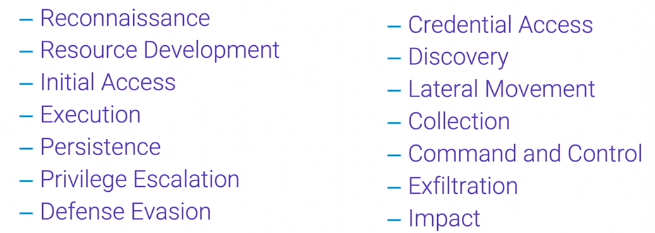
get more detail about the adversary behaviour

e.g:

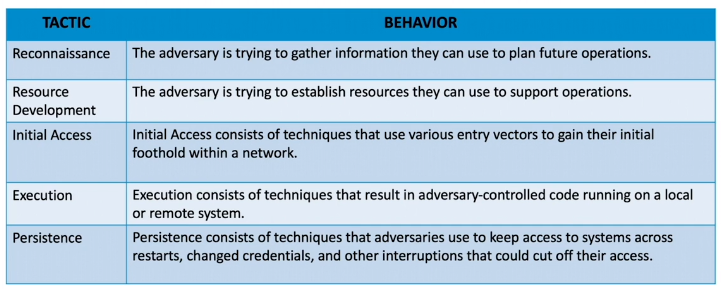
search for more detail about SOCKS5 , what is the default service on port 1913 etc...

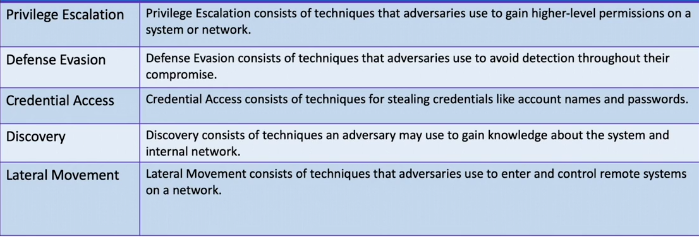
**2) Translting behaviour in to tactics:**

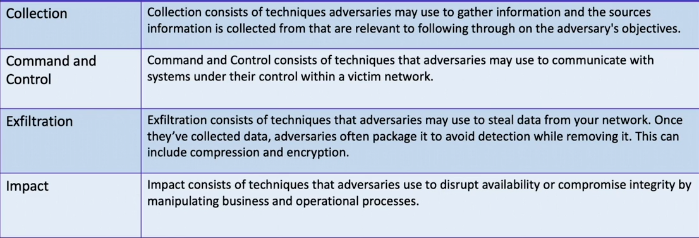
There are 14 Tactics in ATT&CK framework





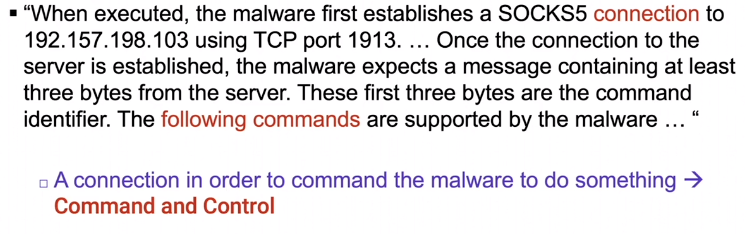




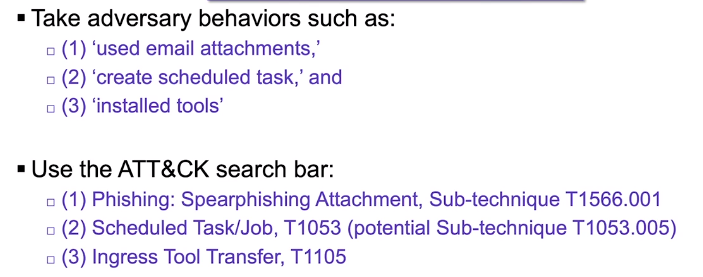


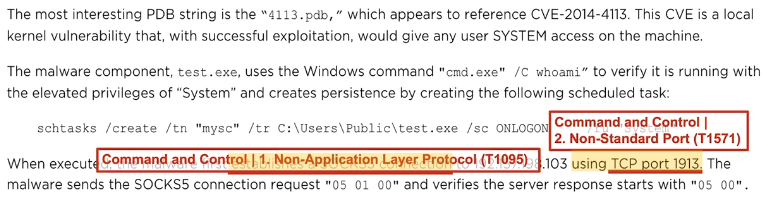
**based onthese 14 tactics, the differnt adversaries behaviour can be mapped to one of the tactics**

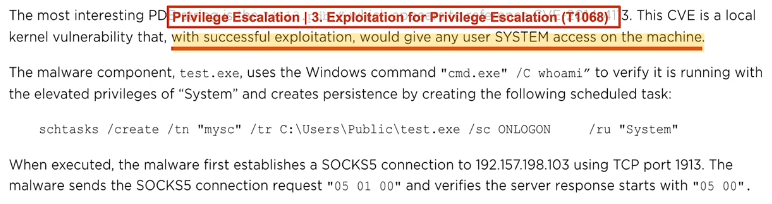
**e.g:**

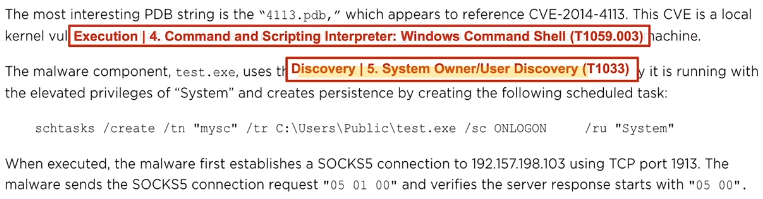
****

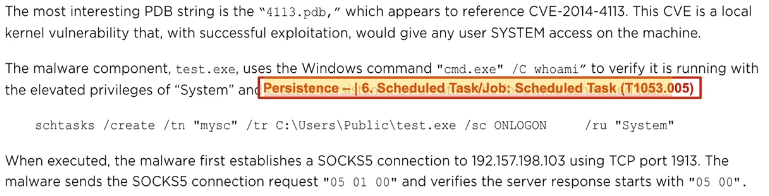
**3) Identify technique and sub techniques:**

****

****

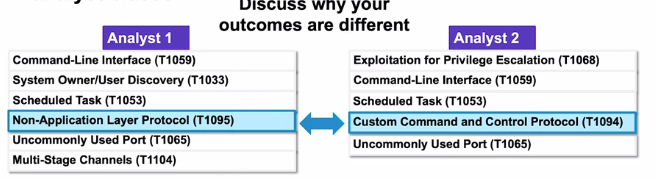
****

****

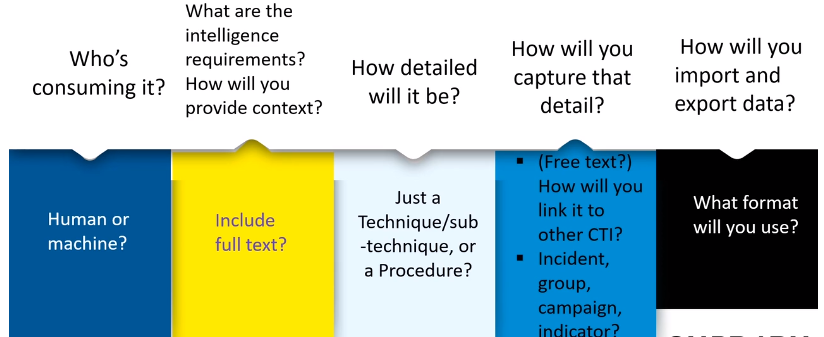
****

**4) compare result with other analysts**

**based on the experience difference analyst may have identified different techniques for the behaviour.**

****

**Storing ATT&CK mapped data:**

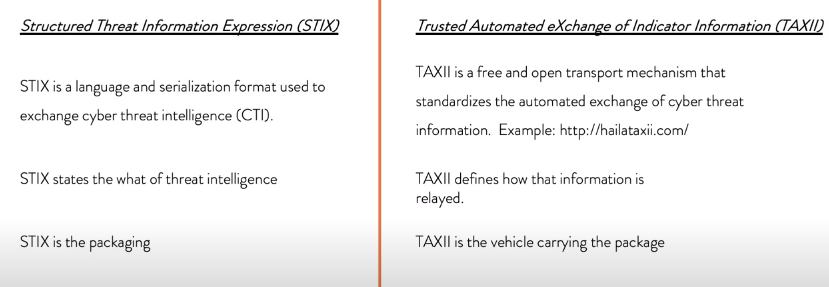
****

MISP is short for Malware Information Sharing Platform. It helps with sharing threat data which can be used by defenders and malware researchers.

**Some known Threat intelligence websites:**



Threat intelligence Exchange:



STIX format:

