Converting ATT&CK Playbooks to Incident Response – Homework

**What key evolutions happened with this campaign in its 4 main iterations?**

* Launched phishing emails
  + They continued to rely on phishing as their main source of luring the victim
  + They also relied on having the victim click on their files
* Sofacy used updated versions of tools seen before in the industry
* Eventually they faced failure by their code being unable to execute (mis-coded)
* They are still continuing to launch attacks (with their malware and techniques evolving) primarily at NATO-aligned states

**What datasets/data feeds would we need to have coming into the SIEM to detect SOFACY?**

* Windows event logs
  + Monitor processes and command line arguments
  + Event logging for task creation/modification
  + Changed/added registry keys
  + Emails logs (?)

**Would we use static correlation or user/entity behavior analytics, or both?**

For static - list how we could write a SIEM rule (refer to security event correlation documentation from prior class)

For U/EBA – list what behaviors we would be interested in defining, and what populations of interest we would need to create (i.e. privileged users)

If both, how will the static content and the U/EBA models interact?

The static content will give us relevant data on what suspicious activity the ‘user’ has done.

The U/EBA model will then assign points to activities that it deems suspicious or out of the ordinary for our ‘user’. If the malware is able to bypass U/EBA, we will have the static content which allows us to trace backwards to find the root cause of the problem (and also what the adversary has done from there). If the U/EBA model did not detect anything, the static content also serves as another means of detection. If an analyst fails to determine any pattern in the static content, then the U/EBA model could help with detection.

The U/EBA model could be created in a way such that they interact with the static content to piece together whether these activities map to patterns seen in previous forms of cyber-attacks.

**Thinking proactively, if we had some level of confidence that SOFACY was active in our environment, list and prioritise (triage) what incident response activities we would want to carry out?**

* Detect where the source of attack is coming from i.e. it could be a .exe file downloaded from an email
* From there, if the attacker is still in our system we contain them if we are able to (maybe through disabling network access from infected PCs)
* If the attacker has little control over our system, we would perhaps allow them to continue their moves to get a grasp on what their motive is and what methods they are using
* Recover the accounts/PCs that were compromised by removing all means that were used to gain access (e.g. backdoor access) and purge the attacker from system
* Identify what the adversary has compromised and also get some depth on the methods they employed to achieve it
* Begin a write up of a report detailing the breach
* Formulate plans to better prevent the system from a breach happening again in the future

**How could we work ahead of the adversary? List some specific technical controls you would work with the IT/tech teams to implement in order to prevent key SOFACY techniques.**

We know that SOFACY is very reliant on using spear phishing attachments as a means to get into the system. As such a preventative measure would be related to email control, namely we could:

* Using network intrusion prevention to remove links and attachments from emails
* Train users to be vary of emails

Next we have seen that SOFACY attach malware with the emails. If we assume our user is going to eventually fall for the phishing emails, we need to also employ a prevention layer here, namely:

* Use antivirus and antimalware
* Restrict some web-based content from being downloaded