Converting ATT&CK Playbooks to Incident Response

Technique Evolution

Evolution:
In general, the techniques used by Sofacy for attack and defense strategy tend to vary between iterations. In the first attack, there is a balance of installations for execution, persistence, privilege escalation and defense evasion. For example, they use logon scripts for persistence, process injection for privilege escalation, using software packing for defense evasion etc. However, the middle two attacks tend to be more aggressive in the sense that they focus on execution. Upon the failure of the Powershell scripts in the third iteration, the fourth attack returns to a strategy that uses more defense evasion techniques like template injection and registry modification. Likewise, the command and control techniques change from iteration to iteration. These evolving techniques suggest that Sofacy is an entity that is highly motivated, funded and makes attack decisions according to the intel they receive.

Patterns:
Conversely, Sofacy's initial access methods and exfiltration/collection strategies tend to always employ similar tactics, indicating that success is continually associated with them. In every attack, spear phishing attachments for initial access. Likewise, upon successful compromise, screen capture, system information discovery, process discovery and remote file copy are consistently used to exfiltrate information about the victim.

Data Feeds

Based on the techniques that reoccur, an entity wishing to protect against this attack would make the following additions to their SIEM system:

- Spear Phishing:
    - Network intrusion detection system (detect spear phishing in transit).
    - Mail server (detect malicious emails in the inbox).
- User execution:
    - Anti-virus: Detect malicious files upon download.
    - Process monitoring: Detect activity once file is opened and log it.
- Standard application layer protocol:
    - Packet capture
    - Log process use of network (both used to detect unusual network activity)
- Remote file copy:
    - As before, analyse network activity
    - File monitoring logs (Especially those created or transferred across SMB)
- Screen capture:
    - Not enough information on Sofacy's particular method of screen capture to make a decision.

    - File monitoring is a generic approach, but may be difficult to monitor, especially with large volumes of file being produced.
- System information discovery:
    - Process monitoring logs
    - Command line monitoring logs
    - Historically, Sofacy achieved system information discovery by running C# and through the command line ‘systeminfo’ command.
- Process discovery
    - The same as system information discovery. Both C# and the command line were used to learn about the current processes.

Static Analysis & UEBA

It would seem that both static analysis and UEBA are both needed. Static analysis alters our data model to account for attacks that are similar to that of Sofacy, while the UEBA approach helps our technology determine whether an activity is normal behaviour for specific groups of people.

Static Analysis:
We can start writing rules based on the past data that we have collected, observing what activities happen consistently and what order they appear to happen in. We can take multiple events that have occurred (based on log data) and create a rule.

E.g. We can create an alert rule for spear phishing attachments and user execution when:
- We can detect the packets coming from an unknown IP address (router)
- Track the email come in through the firewall (firewall)
- Track certain process execution as a result of opening/downloading the attachment.

UEBA:
- Detect certain script execution. Certain users of a company don’t need to be running scripts. E.g. If an employee from finance started running PowerShell scripts when they didn’t usually, this would be suspicious activity. Script execution should lie mainly with IT departments. Also need to monitor the activity admins to ensure that execution activity is not unusual.
- Monitor where certain files are copied remotely from. E.g. If HR usually only copies files from the H Drive. This would define their normal activity regarding remotely copied files.
- Monitor who is accessing system and process information. Usually only IT and infrastructure teams will require this information.

Incident Response

- Identify where the initial breach occurred and trace logs to track where the malware has affected. Use the playbook to guide where to look and what to look for.
- If more than one machine or system is compromised, treat entities with the highest privileges first.
- Deny command and control:

        - Use network intrusion prevention to mitigate remote file copying and registering domains via standard application layer protocol.
        - Delete the newly registered domains and any new files remotely copied.
- Deny persistence:
    - Search for hidden logon scripts (batch files) that cause persistence and remove them from the machine(s).
    - Delete the scripts that were added from remote file copying.
    - Check for registry keys that allow for persistence.

Prevention

- Use anti-malware software to detect spear phishing emails.
- Restrict write access to logon script to administrators.
- Use network intrusion prevention systems to scan for malicious downloads and remote file copying. Block downloads if they try to be executed by the user. Educate users on the awareness of malicious downloads.