Extracting TTPs from Threat Reports Template

In the field, real intelligence for CTE squads are requested from organizations like NTOC, but because of the availability, reports generated for the general public are used in this exercise. This exercise exposes students to a publicly available report on APT30 and requires extraction of information from the reports that could be used to create TEAs.

|  |  |
| --- | --- |
| **Step** | **Action** |
| 1 | Review the APT30 pdf located on the student share. It is also available at:  https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf |
| 2 | Find the “Key Findings” section of the report on page 4. What suite of tools was used for their long-term mission? |
| 3 | What domains has APT30 been known to use? |
| 4 | What are these domains used for? |
| 5 | To emulate the threat, what malware tools would a CTE squad need? |
| 6 | Does APT30 develop some of their own tools? |
| 7 | Choose a tool or technique mentioned in the report and describe how the CTE squad could emulate the tool or technique. |