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?  suite of tools includes downloaders, backdoors, a central controller, and several components designed to infect removable drives and cross air-gapped networks to steal data  BACKSPACe backdoor (also known as “Lecna”)  **Backspace; Neteagel; shipshape; Flashflood** |
| 3 | What domains has APT30 been known to use?  km-nyc.com  km153.com |
| 4 | What are these domains used for?  for use with malware command and control (C2) |
| 5 | To emulate the threat, what malware tools would a CTE squad need?  A script that will download commands, do file manipulation. |
| 6 | Does APT30 develop some of their own tools?  YES.  The group (or the developers supporting them) systematically labels and keeps track of their malware versioning. |
| 7 | Choose a tool or technique mentioned in the report and describe how the CTE squad could emulate the tool or technique.  A script that beacons out every so often and then downloads a command from a stage 2 C2 would replicate the Backspace (NetEagle Remote Control System ) tool  A second custom script can emulate SHIPHAPE as well. You can create a script to look for particular files and copy them over to an external drive, hide them and change the extension. |