This process describes usage of "ETS: malware and tools" tab.

Start

1. Malware/tool sample identified

2. Is this sample (hash) already in the ETS? — Yes / No

3. New details about sample available? — Yes / No

4. Document sample details in ETS

5. Sample already available? — Yes / No

6. Is it possible to extract the sample? — Yes / No

7. Is it a known hash? — Yes / No

8. Ask RE team to extract sample from VT

9. Place sample (zip + password) to "Case Folder/ Malware"

10. Is the behaviour of the sample known? — Yes / No

11. Sample obtained? — Yes / No

12. Submit sample to IMPE Sandbox

13. Sufficient details about sample obtained? — Yes / No

14. Engage RE team

15.1. Create RE Resilient ticket

15.2. Create Slack thread for this sample providing basic details such as name hash.

15.3. Notify RE analyst on slack that you have new sample or notify Anne that you need analyst assigned.

16. Summarise the sample in the Description field in ETS

17. Update "Sample Status" in ETS

18. Add the system name in the "Systems" column for this malware sample

19. Add the full path to "Full paths" in ETS

End