Einführung in Prozesse

Bitte schau das Youtube-Video “Malware Hunting with Mark Russinovich and the Sysinternals Tools” an. Für diese Stunde sind nur die ersten 51 Minuten bis – unwanted Software – relevant.

Video-URL: <https://www.youtube.com/watch?v=vW8eAqZyWeo>

**Beantworte die nachfolgenden Fragen, indem du deine Antwort direkt unter die Frage schreibst. Schicke das Work-Dokument bis Montagabend, 25.1.2021 an** [**Ber@htlwrn.ac.at**](mailto:Ber@htlwrn.ac.at)

1. **Welche 6 Schritte solltest du vornehmen, wenn due eine Malware entfernen willst**
   1. Disconnect from Network
   2. Identify malicious processes and drivers
   3. Terminate identfied processes
   4. Identify and delete malware autostarts
   5. Delete malware files
   6. Reboot and repeat
2. **Im Process-Explorer gibt es zwei vorherrschende Farben hellblau und rosa. Was bedeuten diese?**
   1. Rosa: Hosts Windows Services
   2. Hellblau: Running as use
3. **Gibt es im Process-Explorer unter Windows 10 einen Job?**
4. **Was sind „packed Processes“?**
   1. Kann compressed oder encrypted heißen
5. **Worum handelt es sich bei dem Prozess SVCHOST.exe?**
   1. Hostet „Windows Image Acquisition“
6. **Werden immer alle Prozess im Process Explorer angezeigt? Falls nein, dann nenne einen derartigen Prozess und erkläre, warum dieser nicht angezeigt wurde?**
   1. Ein Proess kann so schnell ablaufen, dass er zwischen den Aktualisierungen vom Process Explorer startet und ended -> Wir nicht erkannt
7. **Welche Möglichkeiten stellt der Process Explorer zur Verfügung, um bösartige Prozesse zu erkennen?**
   1. Doppelklick auf den Prozess und „Verify“ drücken, alle Microsoft Prozessen müssen Verified sein
   2. Die Verified Signers column aktivieren, dann Optionen und Verify Image Signatures
   3. Die Virus Total spalte hinzufügen, dann Optionen und unter VirusTotal.com, CheckVirusTotal.com
   4. In CMD: sigcheck -e -u -vr -s c:\
   5. Unter Strings nach merkwürdigen URL’s schaun
8. **Wozu dient die DLL View?**
   1. CTRL+D, Automated Verified Signature checks und Virus Total checks auf allen dll’s