Indicators of Compromise Checklist

Version 1.2 – Updated 8/4/2019

(Please note – this is not an all-inclusive list):

- Web based logins through Advapi process.
- Presence of advapi32.dll from spawned processes.
- Unauthorized users created with elevated privileges.
- Outbound web traffic to ports 445/447/449/8082/16993 (especially to international IP addresses).
- Traffic to or from Pastebin.com (104.20.209.21) in the previous two weeks.
- Any Anti-Virus hits for either Trickbot or Emotet signatures.
- Spike in phishing emails over the past 2 months.
- Unusual RDP traffic (Continuous connections through LogMeIn or TeamViewer).
- Installed services and scheduled tasks with unusual names / paths.
- Unusual files in user roaming directories.
- Attempted connections to .onion sites
- Presence of tiki.exe in startup programs
- Unauthorized presence or use Ccleaner.exe0
- Presence of tiki.exe, id_up.exe or wdcsam.inf.2823sf8551
- Connections to: 84.146.54.187, 75.147.173.236, 218.16.120.253, 170.238.117.187, 195.123.237.129, 194.5.250.123, 85.204.116.158, 31.184.254.18 or 186.10.243.70
- Hashes to watch for:
    - MD5 d41d8cd98f00b204e9800998ecf8427e
    - SHA1 da39a3ee5e6b4b0d3255bfef95601890afd80709
    - SHA256 e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855