TFlower (Malware Family)

By Fraunhofer FKIE

TFlower is a new ransomware targeting mostly corporate networks discovered in August, 2019. It is reportedly installed on networks by attackers after they gain access via RDP. TFlower displays a console showing activity being performed by the ransomware when it encrypts a machine, further indicating that this ransomware is triggered by the attacker post compromise, similar to Samsam/Samas in terms of TTP. Once encryption is started, the ransomware will conduct a status report to an apparently hard-coded C2. Shadow copies are deleted and the Windows 10 repair environment is disabled by this ransomware. This malware also will terminate any running Outlook.exe process so that the mail files can be encrypted. This ransomware does not add an extention to encrypted files, but prepends the marker "*tflower" and what may be the encrypted encryption key for the file to each affected file. Once encryption is completed, another status report is sent to the C2 server.

▶ [TLP:WHITE] win_tflower_auto (20251219 | Detects win.tflower.)
