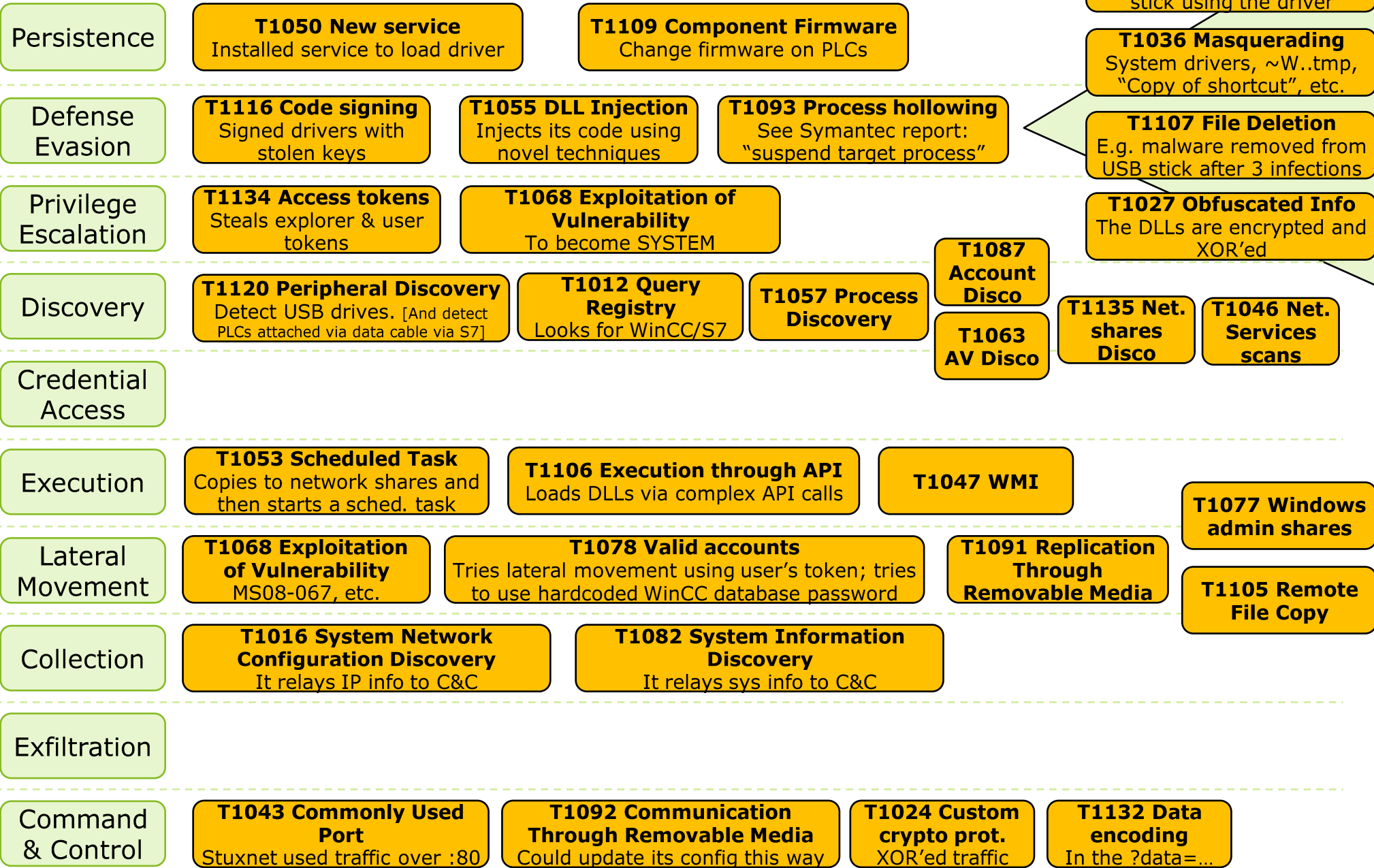


# Which ATT&CK techniques were used in Stuxnet?



**T1014 Rootkit**  
Hide the files from the USB stick using the driver

**T1036 Masquerading**  
System drivers, ~W..tmp, "Copy of shortcut", etc.

**T1107 File Deletion**  
E.g. malware removed from USB stick after 3 infections

**T1027 Obfuscated Info**  
The DLLs are encrypted and XOR'ed

**T1077 Windows admin shares**

**T1105 Remote File Copy**