Which ATT&CK techniques were used in Stuxnet?

Persistence

T1050 New serviceInstalled service to load driver

T1109 Component Firmware
Change firmware on PLCs

Hide the files from the USB stick using the driver

T1036 Masquerading

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

T1014 Rootkit

Defense Evasion

T1116 Code signing
Signed drivers with
stolen keys

T1055 DLL Injection
Injects its code using
novel techniques

T1093 Process hollowing
See Symantec report:
"suspend target process"

T1107 File Deletion

E.g. malware removed from USB stick after 3 infections

Privilege Escalation T1134 Access tokens
Steals explorer & user
tokens

T1068 Exploitation of Vulnerability To become SYSTEM T1027 Obfuscated Info
The DLLs are encrypted and
XOR'ed

Discovery

T1120 Peripheral DiscoveryDetect USB drives. [And detect
PLCs attached via data cable via S7]

T1012 Query Registry Looks for WinCC/S7

T1057 Process
Discovery

Account Disco T1135 I share

T1135 Net. shares Disco

T1046 Net. Services scans

Credential Access

Execution

T1053 Scheduled Task
Copies to network shares and
then starts a sched. task

T1106 Execution through API Loads DLLs via complex API calls

T1047 WMI

T1087

AV Disco

T1077 Windows admin shares

Lateral Movement T1068 Exploitation of Vulnerability MS08-067, etc. T1078 Valid accounts

Tries lateral movement using user's token; tries to use hardcoded WinCC database password

T1091 Replication
Through
Removable Media

T1105 Remote File Copy

Collection

T1016 System Network Configuration Discovery It relays IP info to C&C T1082 System Information
Discovery
It relays sys info to C&C

Exfiltration

Command & Control

T1043 Commonly Used
Port
Stuxnet used traffic over :80

T1092 Communication
Through Removable Media
Could update its config this way

T1024 Custom crypto prot. XOR'ed traffic

T1132 Data encoding In the ?data=.