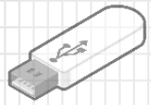
CVE
WORM
MIDM (OPTIONAL)
ROOT-KIT



CVE-2010-2568

COPY TO SHARE(S)

wtr4141.tmp
LOADLIBRARY()

HOOK

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Z|w|M|a|p|V|i|e|w|O|f|S|e|c|t|i|o|n|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Z|w|C|r|e|a|t|e|S|e|c|t|i|o|n|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Z|w|O|p|e|n|F|i|l|e|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+-+-+
|Z|w|C|l|o|s|e|
+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Z|w|Q|u|e|r|y|A|t|t|r|i|b|u|t|e|s|F|i|l|e|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Z|w|Q|u|e|r|y|S|e|c|t|i|o|n|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

mrxcls[DQ].sys INJECTS

lsass.exe
symantec
winlogon.exe
svchost.exe
explorer.exe

Propagate to find SIMATIC S7 PLC

```
++++++++++++++++++++ X ++++++++++++++++++++
[0014FA40]->     Realtek Semiconductor Corp
[0014FA54]->     VeriSign Class 3 Code Signing 2004 CA
[0014FA58]->     Realtek Semiconductor Corp
[0014FA44]->     (null)
[0014FA48]->     http://www.realtek.com
[01202180]->     5e 6d dc 87 37 50 82 84 58 14 f4 42 d1 d8 2a 25
```

- LNK exploit
- Print-spooler (computers w/shared printer)
- Task scheduler (privilege escalation)
- Windows keyboard (privilege escalation)
- Network shares

```
|URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
(138)
00 00 00 44 FF 53 4D 42 75 00 00 00 00 18 01 28        ...D.SMBu......(
00 00 00 00 00 00 00 00 00 00 00 00 00 00 0A 6A        ...............j
01 08 0C 08 04 FF 00 00 00 00 00 01 00 19 00 00        ................
5C 5C 31 30 2E 30 2E 30 2E 31 38 38 5C 49 50 43        \\10.0.0.188\IPC
24 00 3F 3F 3F 3F 3F 00                                $.?????.
```

```
00 00 00 5C FF 53 4D 42 A2 00 00 00 00 18 01 28        ...\.SMB.......(
00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 0A 6A        ...............j
01 08 0C 08 18 FF 00 00 00 00 08 00 16 00 00 00        ................
00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00        ................
00 00 00 00 07 00 00 00 01 00 00 00 00 00 00 00        ................
02 00 00 00 00 09 00 5C 73 70 6F 6F 6C 73 73 00        .......\spoolss.
```

s7otbxdx[S7].dll is replaced

STEP[7]
SIMATIC WinCC

Drops the programming logic
PLC is connected to the right HARDWARE.

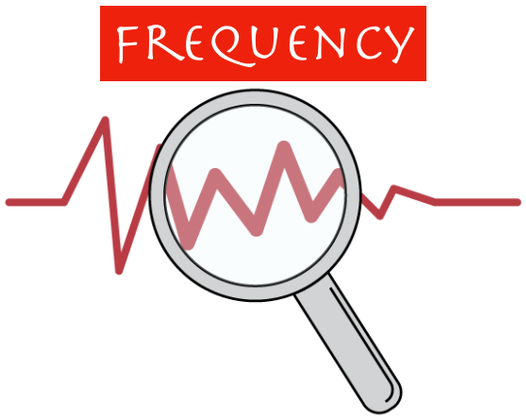
WinCC = operate + monitor

Simatic MANAGER to integrate Network and hardware config, also DB and archiving

S7sCL programming language -> MC7 LOW-LEVEL

Sends data back to reporting system

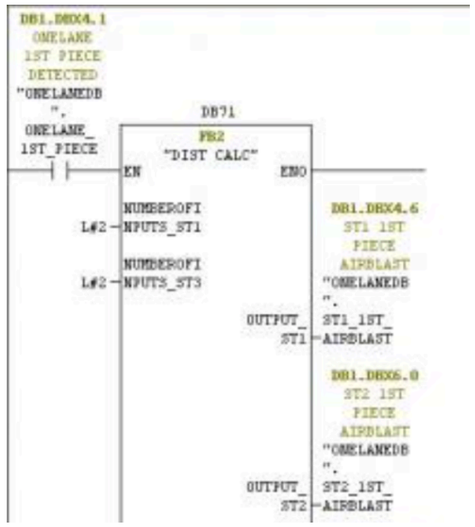
Continue



Hardcoded DB PASSWORD
PASSWORD vulnerability
Carries DB [N] to replace the PLC logic {DATA FILES}

```
"BLK_WRITE, len=%d
```

Address	Name	Type	Initial value	Comment
0.0		STRUCT		
+0.0	DB_VAR	INT	0	Temporary placeholder variable
=2.0		END_STRUCT		



SABOTAGE

CENTRIFUGE