Stuxnet?

A sophisticated worm designed to target only specific Siemens SCADA systems.

Why they can't be detected?

They had digital certificates for it's modules signed by reputed companies.

Capabilities?

exploited multiple 0-day vulnerabilities
- → modified system libraries
- → attacking Step 7 installations
- → running a RPC server

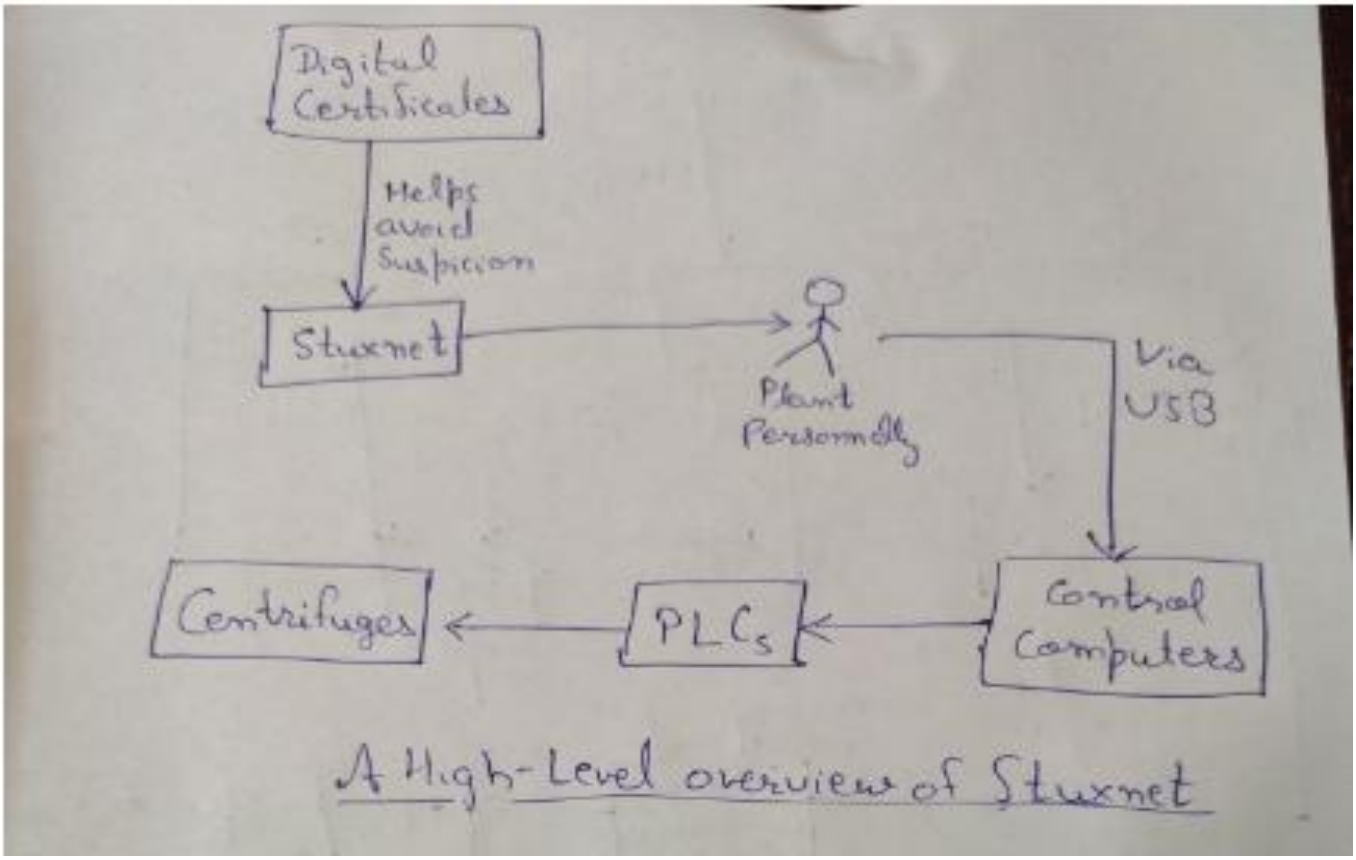
Installed signed drives on windows OS.

Target?

PLCs (Programmable Logic Controllers)
- → special purpose computers used for controlling electronic devices or systems, such as industrial systems.

PLCs are connected to computers that control and monitor them, & typically neither are connected to the Internet.

∴ It has to be in contact with those computers, physically, it means, via USB flash drives or one can introduce USB to the control systems.



A High-Level overview of Stuxnet

Versions? Change upon time?

→ Older versions use an autorun.inf file vulnerability.

→ autorun.inf file

This file causes Windows to automatically run a file on removable media when that media is inserted into a computer.

So, instead of separate file, Stuxnet inserted the code into autorun.inf file along with valid commands to infect computer. Windows ignored the Stuxnet data portion, since it ignores invalid commands in autorun.inf file.

→ recent versions use Windows .LNK vulnerability.

→ .LNK vulnerability

LNK is a file extension for a shortcut file used by MS Windows to point to an executable file, instead of having to navigate to the executable. .LNK files contain some basic properties, such as the path to the executable file and the "Start-IN" directory. LNK files use a curled arrow to indicate they are shortcuts, and the file extension is hidden (even after disabling "Hide extensions for known file types" in Windows Explorer).

When an infected USB is inserted it copies Stuxnet to the drive. Interestingly, an existing copy of stuxnet on the external drive will be removed if that drive has already infected three computers.

In addition to the Stuxnet DLL & a loader for it, the malware creates four .lnk files on the removable drive. They are used to execute the loader when a user views the drive, four

are needed in order to target different versions of Windows

→ Via Step 7 projects

On an infected computer, Stuxnet tries to/does modify DLLs (Windows Dynamic Link Library; a library of shared objects: code, data, resources) and an .exe file in the WinCC Semantic manager, so that they execute Stuxnet code as well. The additional code will infilterate Stuxnet into Step 7 project directories.

→ Via WinCC

Stuxnet searches for computer running Siemens WinCC, an interface to their SCADA systems. It connects using a password hardcoded into WinCC, and attacks its database using SQL commands to upload and start a copy of itself on the WinCC computer

→ Via network shares

Stuxnet can use Windows shared folders to propagate itself over a local network. It places a dropper file on any shares on remote computers, and schedules a task to execute it.

→ Via MS10-061 Print Spooler vulnerability

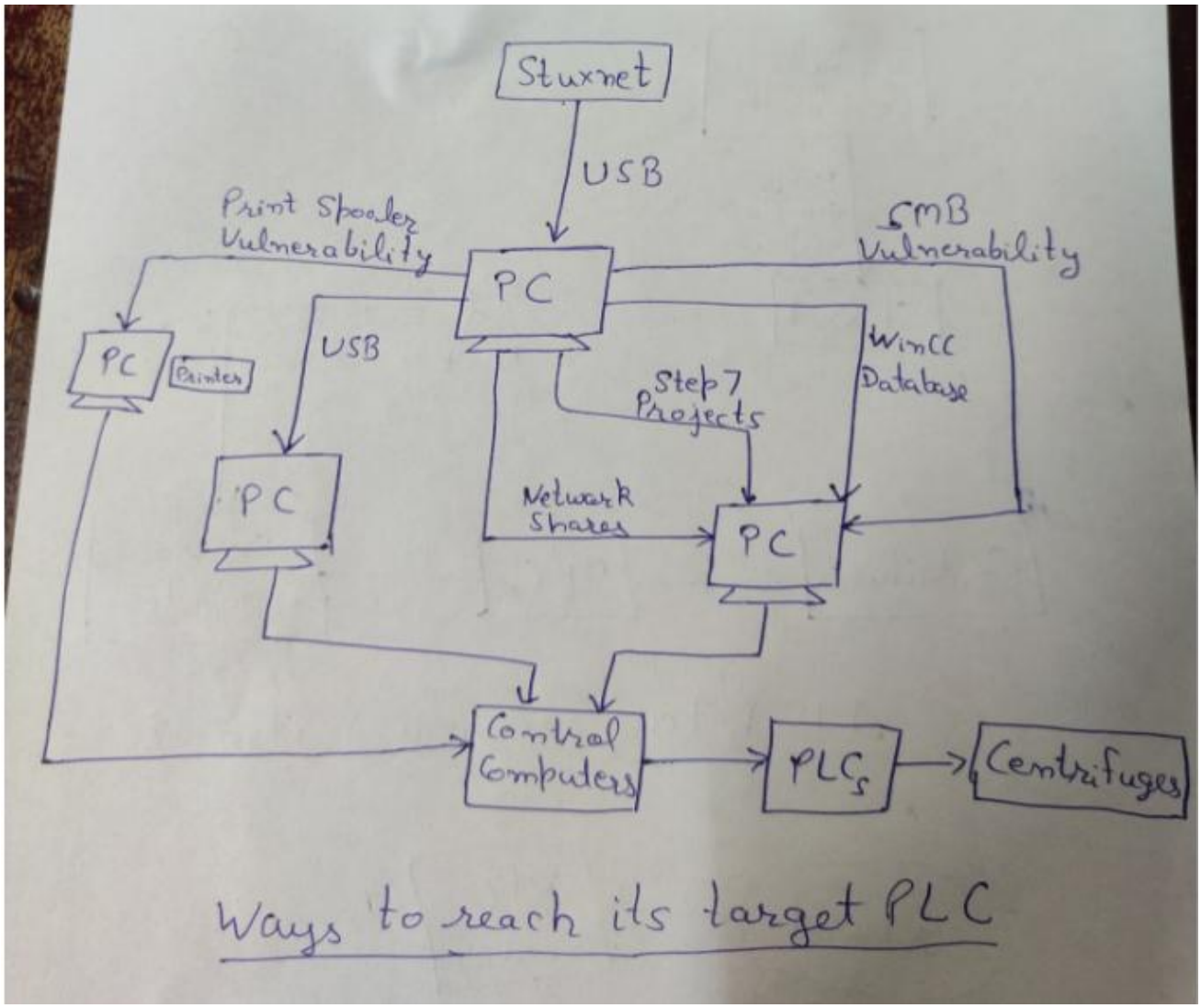
In brief, Stuxnet prints itself (copies itself) into 2 files in the %system% directory on each target machine, using the 0-day privilege escalation. It the executes the dropper file to infect the computer.

→ Via MS08-067 SMB Vulnerability

SMB (Server Message Block)

→ a network communication protocol for providing shared access to files, printers & serial ports between nodes on a network

If a remote computer has MS08-067 SMB vulnerability, Stuxnet can send a malformed path over SMB; this would allow it to execute arbitrary code on the remote machine, thereby propagating itself to it.



Ways to reach its target PLC

What it can do?

Stuxnet's main module consists of both user-mode and Kernel-mode components. The user's mode functions could do:-

- → Inject it into a chosen process add its own code into a running process which results in the execution of that code in the target process address space.
- → check for appropriate platform.
- → escalate privileges
- → install two Kernel-mode drivers, one for running Stuxnet after reboot and the other as a rootkit to hide its files.

Contact with outside world?

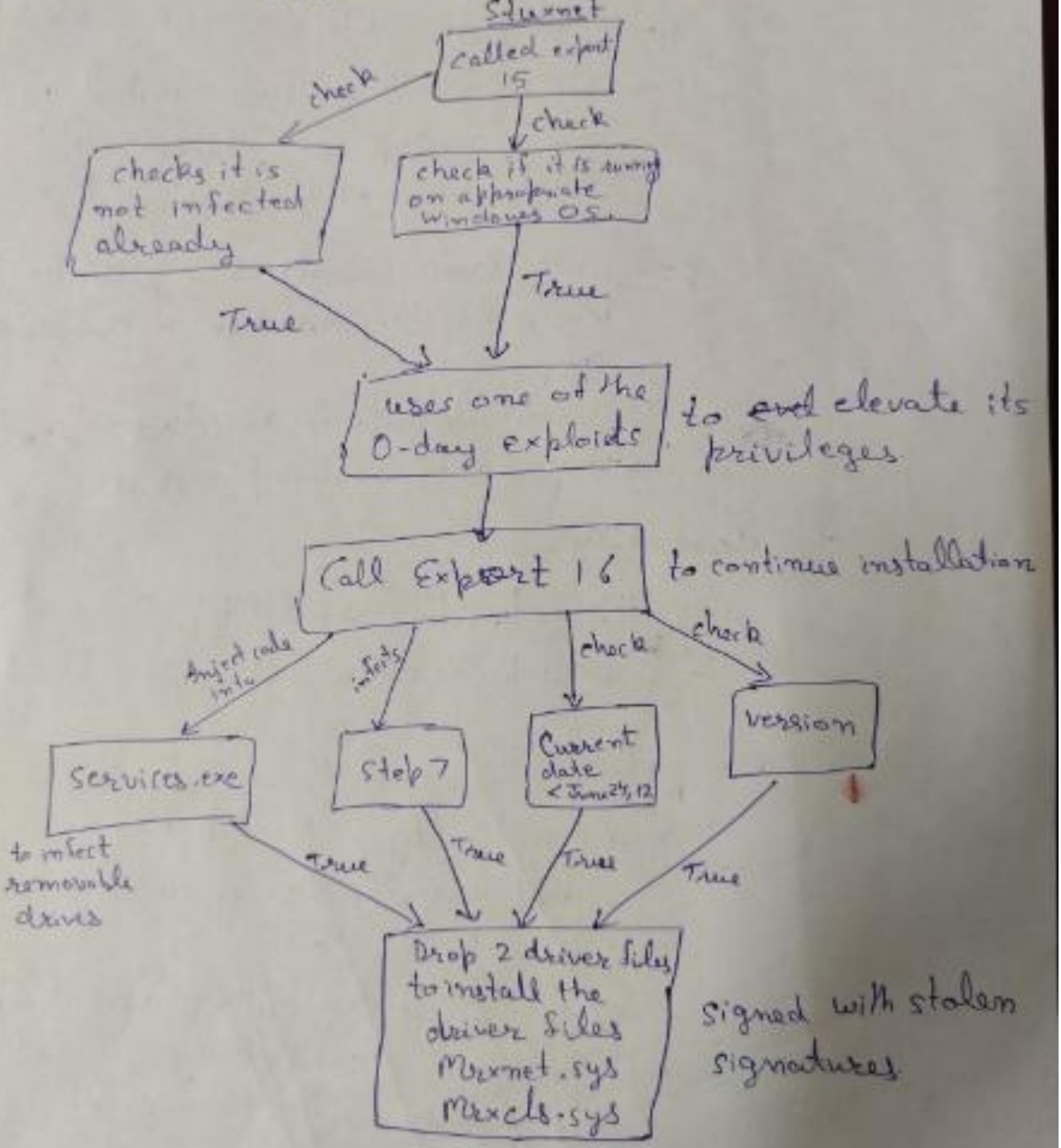
After setting up base in the computer, it tries to contact one of two servers via HTTP:

- → www.mypremierfutbol.com
- → www.todaysfutbol.com

It sends it's IP address, some unknown data, and a payload consisting of, in part, info on the host OS, the host computer name, and domain name, and a flag indicating if Siemens Step 7 or WinCC is installed.

Malware's User Mode

The main module DLL exports 21 functions; Stuxnet by calling export 15.



Kernel-Mode

→ mrxcls.sys

- → Driver signed by a Realtek certificate
- → while installing, it was marked as a boot startup so it starts in the early stages of windows boot.
- → this driver reads a registry key which has been written in the installation step
- → It contains info for injecting Stuxnet images into certain processes.

→ mrxnet.sys

- → It's actually a root kit
- → It had digitally signed certificated signed by Realtek.
- → creates a device object and attaches it to the system's device so that it can monitor all requests sent to those objects.

REFENCES:

- https://isis-online.org/
- https://en.wikipedia.org/wiki/Stuxnet
- https://en.wikipedia.org/wiki/Autorun.inf
- https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067
- https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-046
- https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-061