

stuxnet:

a technical, political, and business analysis

joshua smith
josh@toastresearch.com
2010.10.12



stuxnet: an overview

- what is the purpose of stuxnet?
 - to reprogram industrial control systems (a certain program logic controller in this case)
- what is stuxnet and when was it discovered?
 - malware that was first discovered by security firm virusblokada based in belarus in june of 2010, but thought to have been around since at least june 2009 (possibly earlier)
- why is it any different from other malware?
 - its target(s)
 - its complexity



stuxnet: technical

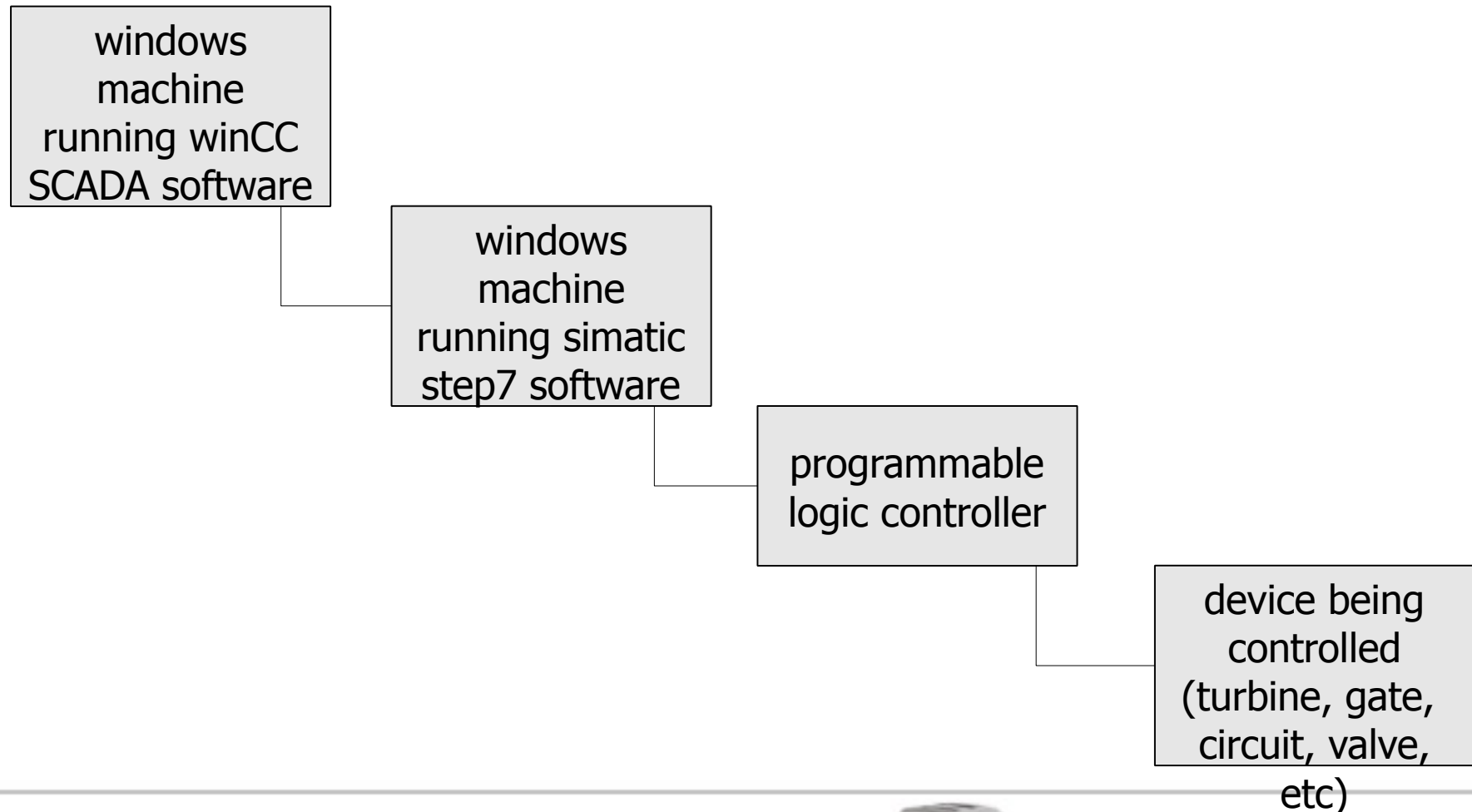
purpose of the technical section

- the players
 - windows (32-bit, 2000 and higher)
 - siemens wincc SCADA system
 - siemens simatic step7 industrial control software
 - programmable logic controller (PLC)



stuxnet: technical

the players in action



stuxnet: technical

what makes stuxnet technically interesting?

- easily the most complex malware ever discovered
 - 4 zero-day exploits used*
 - valid digitally signed drivers
 - first PLC rootkit
 - windows rootkit
 - advanced AV evasion
 - infection mechanisms
 - update mechanisms



stuxnet: technical

how is stuxnet propagated/executed?

- network propagation
 - infecting wincc DB servers*
 - network shares via:
 - wmi
 - scheduled jobs
 - ms10-061 – print spooler vulnerability (0-day: disputed)
 - ms08-067 – windows server services vulnerability (a la conficker)

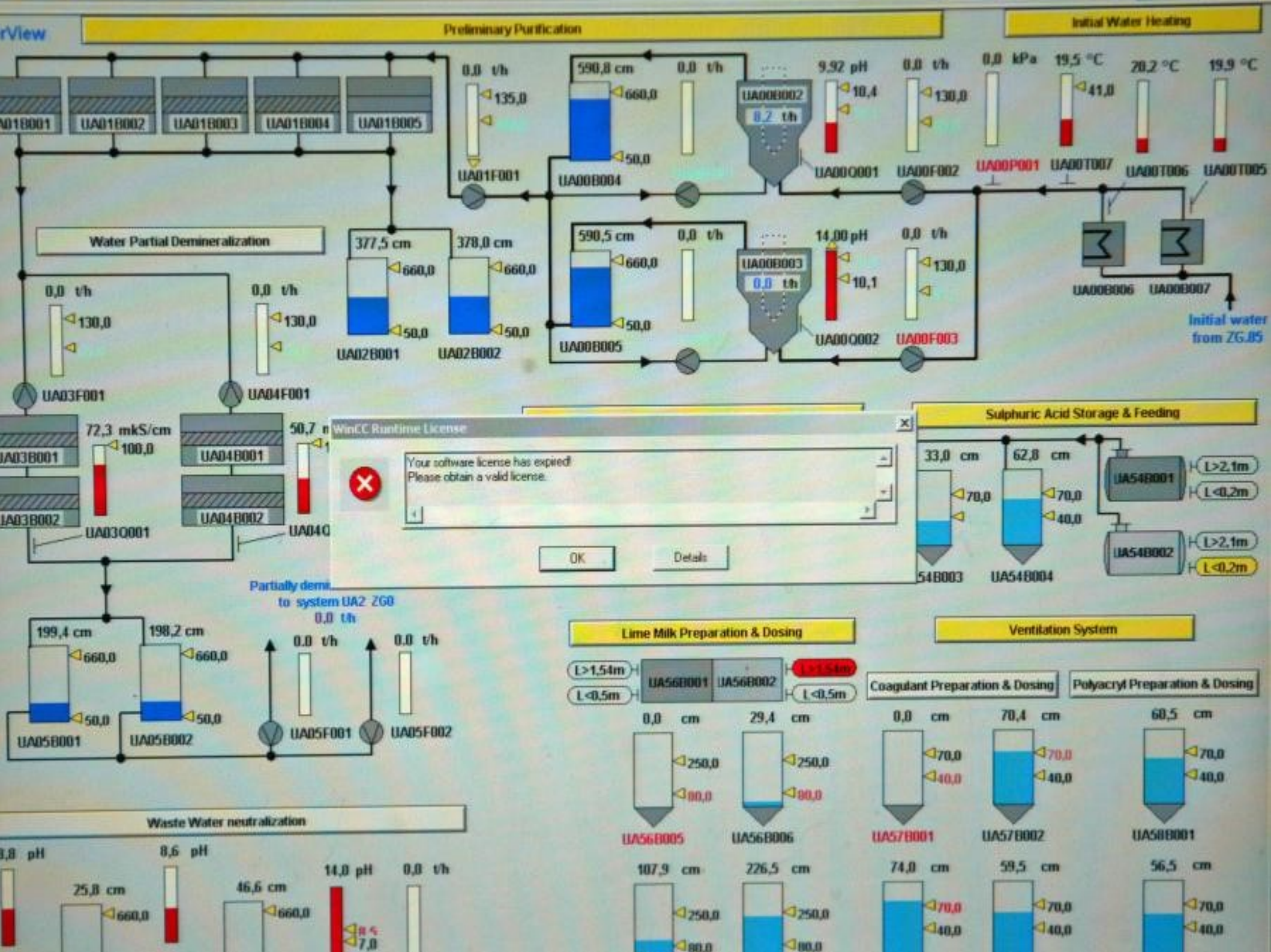


stuxnet: technical

how is stuxnet propagated/executed?

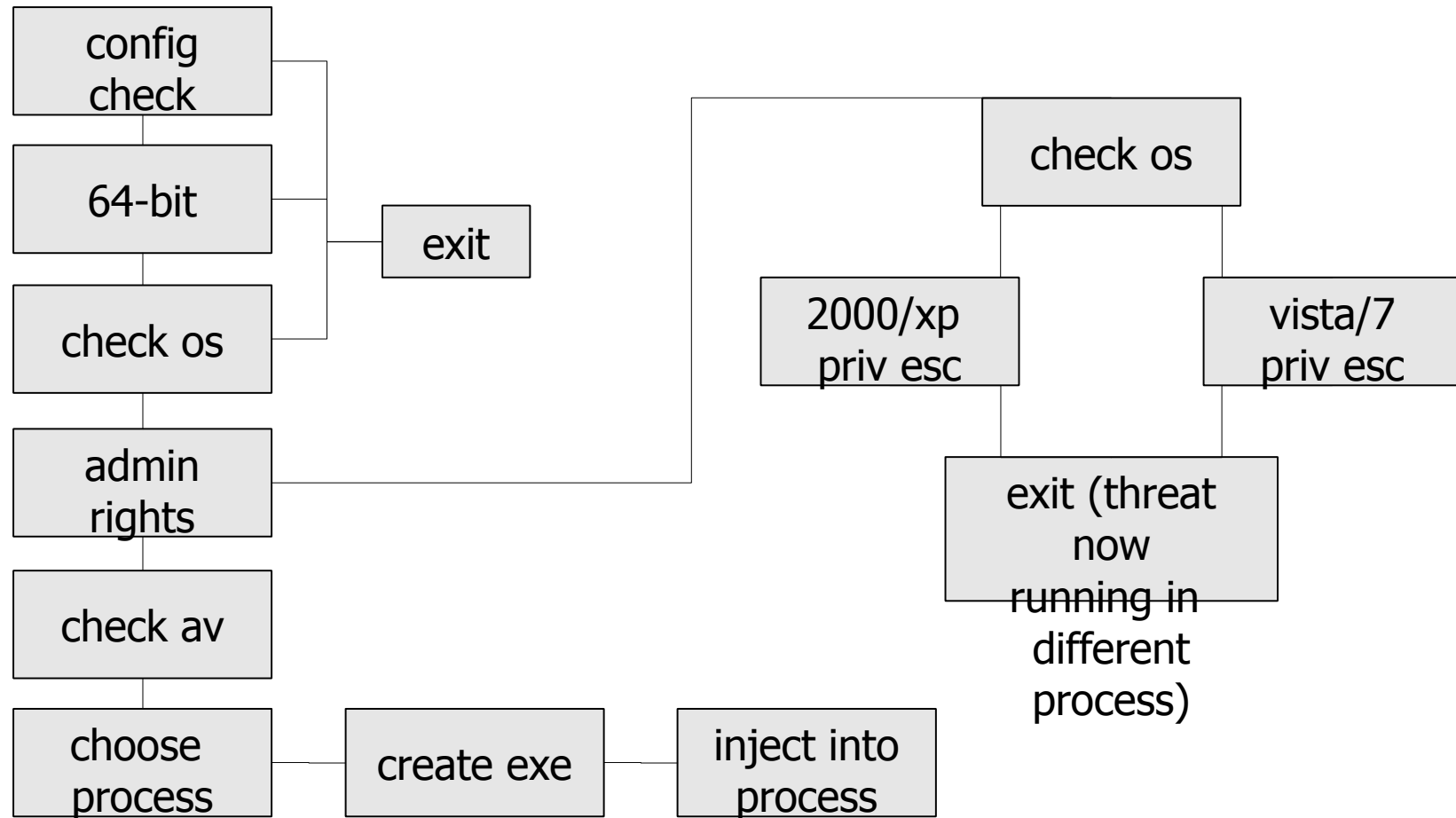
- removable drive propagation
 - ms10-046 – Ink/shortcut vulnerability (0-day)
 - autorun.inf (older version)
- project files
 - step7 project files
 - s7p files
 - mcp files





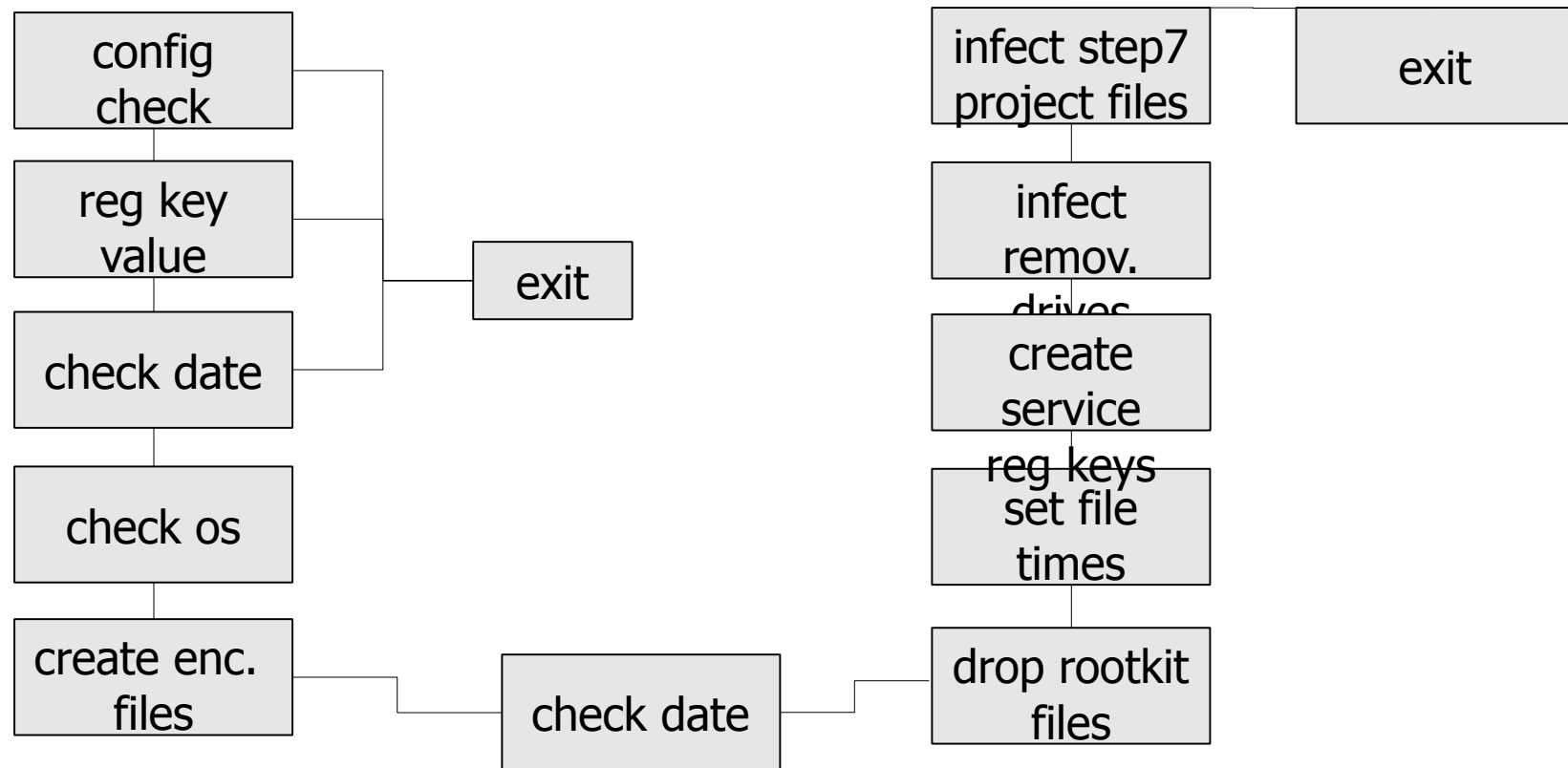
stuxnet: technical

admin rights and injection



stuxnet: technical

installation



stuxnet: technical

persistence

- mrxcls.sys driver set as new system service via reg keys from installation process
- digitally signed with valid certificate
- injects copies of stuxnet into
 - services.exe
 - s7tgtopx.exe (simatic manager)
 - ccprojectmgr.exe (wincc project manager)



stuxnet: technical

command & control

- once stuxnet has gathered desired information, it attempts to contact its command & control if there is an internet connection
 - www.mypremierfutbol.com & www.todaysfutbol.com
 - can be remotely updated and instructed
 - updates can also take place via peer-to-peer communication



stuxnet: technical

hiding itself: the windows rootkit

- mrxnet.sys driver is also set as new system service via reg keys from installation process
- digitally signed with valid certificate
- manages ntfs, fat, and cd-rom devices. it filters out two things
 - files that have a .lnk extension and are 4,171 bytes
 - files named “~wrt[four numbers].tmp”, whose size is between 4Kb and 8Mb and the sum of the four numbers modulo 10 is null



stuxnet: technical

the **really** interesting part: the PLC rootkit

- siemens simatic (step7) programs and controls the PLC
- step7 dll is replaced (s7otbxdx.dll) == all your SCADA are belong to us
 - controls read and write of all code on the PLC



stuxnet: political

- estimated human resources to complete exploit
 - 5-10 people with very advanced skill level in several different areas of exploitation
 - 6 months to a year+ to complete
- it targets SCADA and PLC equipment
- it would require SCADA and PLC equipment to test exploits on (not impossible to get, but not common either)



stuxnet: political

- according to symantec, approximately 60% of all infections worldwide were in iran
- of the infected systems in iran, approx 2/3 had siemens software installed on it (vs. about 10% elsewhere)
- in the driver file, the project path 'b:\myrtus\src\objfre_w2k_x86\i386\guava.pdb' was not removed
 - guavas are in the myrtle (myrtus) family. queen ester was originally named hadassah, which means 'myrtle' in hebrew



stuxnet: political

- "do not infect" registry key is 19790509
 - date first jew in the new ir of iran was executed
- "we came to the conclusion that, for our purposes, a key iranian vulnerability is in its on-line information," said one recently retired israeli security cabinet member, using a generic term for digital networks. "we have acted accordingly."



stuxnet: political

- in july of 2009, the head of iran's atomic energy organization had abruptly resigned for unknown reasons after 12 years on the job
- statistics from 2009 show that the number of enriched centrifuges operational in iran mysteriously declined from about 4,700 to about 3,900
- some speculate that the target was the bushehr nuclear power plant in iran, others point to the natanz facility, a centerfuge plant, that is designed to enrich uranium
- wikileaks article



stuxnet: business

- bad guys now have an excellent blueprint of how to attack SCADA systems
- the biggest business impact of stuxnet today is discussion and awareness
- your company might not be enriching uranium, but you can utilize such a high profile attack to educate and converse with decision makers



stuxnet: business

- practically, things like zeus (now featuring two factor auth solutions) hit the bottom line harder, but stuxnet can get you in the door to discuss
- gary warner has an excellent writeup of a well planned attack on ATM's from a year ago that has some similarities to the stuxnet attack



stuxnet: wrap-up

- conclusion
- questions?

thanks for listening!



stuxnet: references

- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- http://news.cnet.com/8301-27080_3-20018530-245.html
- <http://www.langner.com/en/index.htm>
- <http://www.schneier.com/blog/archives/2010/10/stuxnet.html>
- <http://en.wikipedia.org/wiki/Stuxnet>
- http://news.cnet.com/8301-1009_3-20011095-83.html
- <http://www.wired.com/threatlevel/2010/09/stuxnet/>
- <http://garwarner.blogspot.com/2009/11/9-million-world-wide-bank-robbery.html>
- <http://www.ynetnews.com/articles/0,7340,L-3742960,00.html>



stuxnet: terminology

- SCADA – supervisory control and data acquisition (old terminology)
- DCS – digital control systems (new terminology)
- PLC - programmable logic controller

