First IBM PC virus (1987)

• Propagation method
  • Copies itself into the boot sector
  • Tells the OS that all of the boot sector is “faulty” (so that it won’t list contents to the user)
    - Thus also one of the first examples of a **stealth** virus
  • Intercepts disk read requests for 5.25” floppy drives
    - Sees if the 5th and 6th bytes of the boot sector are 0x1234
    - If so, then it’s already infected, otherwise, infect it

• Payload:
  • Nothing really; goal was just to spread (to show off?)
  • However, it served as the template for future viruses
<table>
<thead>
<tr>
<th>Displacement</th>
<th>Hex codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000:0000</td>
<td>FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 20</td>
</tr>
<tr>
<td>0000:0010</td>
<td>20 20 20 20 20 20 57 65 6C 63 6F 6D 65 74 6F</td>
</tr>
<tr>
<td>0000:0020</td>
<td>20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20</td>
</tr>
<tr>
<td>0000:0030</td>
<td>20 20 20 20 20 20 20 20 20 20 20 20 20 20</td>
</tr>
<tr>
<td>0000:0040</td>
<td>20 20 20 20 20 20 20 20 20 20 20 20 20 20</td>
</tr>
<tr>
<td>0000:0050</td>
<td>20 20 28 63 23 20 39 33 38 36 20 42 61 73 74</td>
</tr>
<tr>
<td>0000:0060</td>
<td>26 20 41 6D 64 61 64 20 20 20 20 20 20 20 20</td>
</tr>
<tr>
<td>0000:0070</td>
<td>64 20 20 20 20 20 20 20 20 20 20 20 20 20 20</td>
</tr>
<tr>
<td>0000:0080</td>
<td>20 42 52 41 49 44 4E 20 20 20 20 20 20 20 20</td>
</tr>
<tr>
<td>0000:0090</td>
<td>53 45 52 56 49 44 45 53 53 30 20 20 20 20 20</td>
</tr>
<tr>
<td>0000:00A0</td>
<td>56 45 41 4B 20 20 20 20 20 20 20 20 20 20 20</td>
</tr>
<tr>
<td>0000:00B0</td>
<td>20 49 51 42 41 4C 20 20 20 20 20 20 20 20 20</td>
</tr>
<tr>
<td>0000:00C0</td>
<td>20 20 20 20 20 20 20 20 20 20 20 20 20 20 20</td>
</tr>
<tr>
<td>0000:00D0</td>
<td>45 20 50 41 44 49 53 54 41 44 4E 20 20 20 20</td>
</tr>
<tr>
<td>0000:00E0</td>
<td>45 20 3A 34 33 30 37 39 33 31 2C 34 34 33 32</td>
</tr>
<tr>
<td>0000:00F0</td>
<td>2C 32 38 30 35 33 30 20 20 20 20 20 20 20 20</td>
</tr>
</tbody>
</table>

**ASCII value**: `0364$ @: @
Welcome to the Dungeon

(c) 1986 Basit & Amjad (put) Ltd.
BRAIN COMPUTER SERVICES..730 N
ZAM BLOCK ALLAMA
IGBAL TOWN
LAHORE
E-PAKISTAN..PHON
E : 430791, 443249
280530.`
ROOTKITS

Malicious code that hides from discovery

• Ways to hide:
  • By intercepting system calls, patching the kernel, etc.
  • Often effectively done by a man in the middle attack

• Rootkit revealer: analyzes the disk offline and through the online system calls, and compares

• Mark Russinovich ran a rootkit revealer and found a rootkit in 2005...
SONY XCP ROOTKIT
Detected 2005
SONY XCP ROOTKIT

Detected 2005

- Goal: keep users from copying copyrighted material
SONY XCP ROOTKIT

Detected 2005

• Goal: keep users from copying copyrighted material

• How it worked:
  • Loaded thanks to autorun.exe on the CD
  • Intercepted read requests for its music files
  • If anyone but Sony’s music player is accessing them, then garble the data
  • Hid itself from the user (to avoid deletion)
SONY XCP ROOTKIT

Detected 2005

• Goal: keep users from copying copyrighted material

• How it worked:
  • Loaded thanks to autorun.exe on the CD
  • Intercepted read requests for its music files
  • If anyone but Sony’s music player is accessing them, then garble the data
  • Hid itself from the user (to avoid deletion)

• How it messed up
  • Morally: violated trust
  • Technically: Hid all files that started with “$sys$”
  • Seriously?: The uninstaller did not check the integrity of the code it downloaded, and would not delete it afterwords.
STUXNET

June 2010

- **Virus** in that it initially spread by infected USB stick
  - Once inside a network, it acted as a **worm**, spreading quickly

- Exploited **four** zero-day exploits
  - Zero-day: Known to only the attacker until the attack
  - Typically, one zero-day is enough to profit
  - Four was unprecedented
    - Immense cost and sophistication on behalf of the attacker

- **Rootkit:** installed **signed** device drivers
  - Thereby avoiding user alert when installing
  - Signed with **certificates stolen** from two Taiwanese CAs
STUXNET: PAYLOAD
STUXNET: PAYLOAD

• Do nothing
STUXNET: PAYLOAD

• Do nothing

• Unless attached to particular models of frequency converter drives that operate at 807-1210Hz
STUXNET: PAYLOAD

- Do nothing

- Unless attached to particular models of frequency converter drives that operate at 807-1210Hz
  - You know, like those in Iran and Finland
STUXNET: PAYLOAD

- Do nothing

- Unless attached to particular models of frequency converter drives that operate at 807-1210Hz
  - You know, like those in Iran and Finland
  - .. those ones that are used to operate centrifuges
STUXNET: PAYLOAD

• Do nothing

• Unless attached to particular models of frequency converter drives that operate at 807-1210Hz
  • You know, like those in Iran and Finland
  • .. those ones that are used to operate centrifuges
  • .. for producing enriched uranium for nuclear weapons
STUXNET: PAYLOAD

• Do nothing

• Unless attached to particular models of frequency converter drives that operate at 807-1210Hz
  • You know, like those in Iran and Finland
  • .. those ones that are used to operate centrifuges
  • .. for producing enriched uranium for nuclear weapons

• In which case, slowly increase the freq to 1410Hz
STUXNET: PAYLOAD

- Do nothing

- Unless attached to particular models of frequency converter drives that operate at 807-1210Hz
  - You know, like those in Iran and Finland
  - .. those ones that are used to operate centrifuges
  - .. for producing enriched uranium for nuclear weapons

- In which case, slowly increase the freq to 1410Hz
  - You know, enough to break the centrifuge
STUXNET: PAYLOAD

- Do nothing

- Unless attached to particular models of frequency converter drives that operate at 807-1210Hz
  - You know, like those in Iran and Finland
  - .. those ones that are used to operate centrifuges
  - .. for producing enriched uranium for nuclear weapons

- In which case, slowly increase the freq to 1410Hz
  - You know, enough to break the centrifuge
  - .. all the while sending “looks good to me” readings to the user
STUXNET: PAYLOAD

- Do nothing

- Unless attached to particular models of frequency converter drives that operate at 807-1210Hz
  - You know, like those in Iran and Finland
  - .. those ones that are used to operate centrifuges
  - .. for producing enriched uranium for nuclear weapons

- In which case, slowly increase the freq to 1410Hz
  - You know, enough to break the centrifuge
  - .. all the while sending “looks good to me” readings to the user
  - .. then drop back to normal range
STUXNET: PAYLOAD

- Targets industrial control systems by overwriting programmable logic boards
- Man-in-the-middle between Windows and Siemens control systems; looked like it was working properly to the operator
- In reality, it sped up and slowed down the motors
- Result: Destroy (or at least decrease the productivity of) nuclear centrifuges
STUXNET: PAYLOAD

• Targets industrial control systems by overwriting programmable logic boards

• Man-in-the-middle between Windows and Siemens control systems; looked like it was working properly to the operator

• In reality, it sped up and slowed down the motors

• Result: Destroy (or at least decrease the productivity of) nuclear centrifuges
**STUXNET: PAYLOAD**

- Targets industrial control systems by overwriting programmable logic boards
- Man-in-the-middle between Windows and Siemens control systems; looked like it was working properly to the operator
- In reality, it sped up and slowed down the motors
- Result: Destroy (or at least decrease the productivity of) nuclear centrifuges
STUXNET: PAYLOAD

• Targets industrial control systems by overwriting programmable logic boards

• Man-in-the-middle between Windows and Siemens control systems; looked like it was working properly to the operator

• In reality, it sped up and slowed down the motors

• Result: Destroy (or at least decrease the productivity of) nuclear centrifuges
STUXNET: PAYLOAD

• Targets industrial control systems by overwriting programmable logic boards

• Man-in-the-middle between Windows and Siemens control systems; looked like it was working properly to the operator

• In reality, it sped up and slowed down the motors

• Result: Destroy (or at least decrease the productivity of) nuclear centrifuges
STUXNET: PAYLOAD

- Targets industrial control systems by overwriting programmable logic boards

- Man-in-the-middle between Windows and Siemens control systems; looked like it was working properly to the operator

- In reality, it sped up and slowed down the motors

- Result: Destroy (or at least decrease the productivity of) nuclear centrifuges
STUXNET: PAYLOAD

- Targets industrial control systems by overwriting programmable logic boards

- Man-in-the-middle between Windows and Siemens control systems; looked like it was working properly to the operator

- In reality, it sped up and slowed down the motors

- Result: Destroy (or at least decrease the productivity of) nuclear centrifuges
STUXNET FALLOUT

• Iran denied they had been hit by Stuxnet

• Then claimed they were, but had contained it

• Understood now that it took out 1k of Iran’s 5k centrifuges

• Security experts believe the U.S. did it (possibly along with Israel) due to its sophistication and cost

• Legitimized cyber warfare
VIRUSES: SUMMARY

• Technological arms race between those who wish to detect and those who wish to evade detection

• Started off innocuously, capable by only a few very clever people

• But viruses have become commoditized; any scriptkiddy can launch one (creation remains hard)

• No longer purely of academic interest
  • Economic pursuits (zero-day markets)
  • Cyber warfare
• Detecting malware in the Android app store
• Lots of drive-by-download work
• Malware distribution networks: use enterprise-wide network traces to detect malware downloads
• Side-channel defenses: Measure, e.g., power consumption of benign vs. malicious code
• Metamorphic arms race