I am a 23-year IT veteran. I am/was hacked. I've seen this hack spread. A few suggestions that need to be looked at to protect the security of our nation's computers.

1. Disable TPM in Bios -- The hackers use this to flash bios to be able to modify system settings to fit their needs. In my case, netboot was enabled (unknowingly) and the system was net boot to a server elsewhere. Protect the way a machine boots. Don't let a virus or a hacker to modify the boot process.

2. Disable Peer to Peer networking. This includes Bonjour, Windows media player, Unity (I believe that's what it is called) on Linux. Also created a peer to peer network of all neighbor systems and had remote access to any/all systems.

3. Prevent certificates being updated from a URL -- from a valid IP only. URLs can be spoofed. IP addresses can't. Therefore, when my system got software updates and updates from apple or microsoft, it was going to a re-directed site. If an IP can be specified, I would highly recommend this.

4. At any given time, have a copy of Arin's DNS records available in hard copy. If all the DNSs (Roots included) get corrupted -- and it's possible, how will we know what the "real" address is for google, or Yahoo....or the Bank for that matter. Fake websites can be established.

5. Educate the public on IP addressing both IP 4 and IP6. The public has little knowledge about this. How are they to know what to look for if they are intruded on. Educating the public on what to look for to me, would be very important. I've seen a hack move around Indianapolis, and some systems people don't even recognize it....and it could go DAYS before it's found.

6. Prevent use of 3G on General internet. With this, Cell phones are able to hack into computers. I know this for a fact as m computer was connected to someone's cell phone. I couldn't stop it. Antivirus didn't look at it....didn't find it.

7. Prevent TVs and Satellites from talking to PCs. Or establish a firefwall for these devices. I saw DSSN protocol on my laptop. (I believe this is the protocol of satellite communication). My laptop was chatting with a satellite -- and I couldn't stop it, couldn't turn it off. Same with the TV. The TV was using the same ports that the rating systems use (G/PG/MA, etc).

8. If there's any open holes, plug them up. Plug up holes for any electronic devices that can be on the internet -- including cars, thermostats, lighting, heating, security cameras. If it's on the internet, it can be hacked. I saw a hack come from a printer/fax -- utilizing the web services on the printer to hack at computers on the network. It would be very hard to detect.

9. Educate IT Staff for what to look for. As a support tech of 23 years, it used to be just strange services and websites that would show signs of hacks, and it has gotten much more sophisticated.

10. Java is bad. I could not get rid of the virus. It used a flaw in Java, flash, and adobe to get in, and I couldn't get rid of it.

11. Eliminate unneeded applications, widgets, etc. These hackers will make use of code and hide inside applications. I saw where graphics (png, bmp) had a 2nd layer to them -- so that once the graphic was opened, the virus was implanted. Facebook is full of them. I figure other graphic sites have them as well.

12. Eliminate contractors. Have the systems people work FOR you. Contractors have no loyalty to a contract house, and therefore don't have loyalty to corporations. Having contractors work on critical and sensitive data is a risk.

If you want more ideas, I have plenty written down. These are just a few of the things

--
Mary C. Anderson

hoosierchick67@gmail.com