Michael Silver

1. Poison Ivy
2. 2005
3. Traced back to China
4. Spread through an email attachment sent to the employees of various corporations. The attachments looked like text files based on their filename and icon, but were actually disguised executable files. An alternate variation included a password protected archive attached to an email that included an executable file that would be run upon entering the password included in the email, disguised to be a security update.
5. Windows
6. Gave full control of the computer “through a backdoor” (smithsonianmag.com), including the ability to use the camera and audio of the computer, in addition to changing, running, copying, or deleting any files.
7. Upon infection, it copies itself into the Windows or Windows\windows32 folder, in addition to adding it into a registry entry to ensure it will start on boot-up of the computer. The virus bypasses the firewall and makes a secure connection with a remote server. The virus allows a person to remotely use the command prompt.
8. Step by step: <http://www.malwareexperts.com/how-to-remove-poison-ivy-virus/>
9. Yes. There are many versions of the poison ivy attack. And in general, there are many different versions of a virus that takes over the whole computer as this virus does.
10. Unknown
11. Not found.

Works Cited

"Backdoor:W32/PoisonIvy." *Backdoor:W32/PoisonIvy*. N.p., n.d. Web. 26 July 2013. <http://www.f-secure.com/v-descs/backdoor\_w32\_poisonivy.shtml>.

"How to Remove Poison Ivy Virus." *MalwareEXPERTS RSS*. N.p., n.d. Web. 26 July 2013. <http://www.malwareexperts.com/how-to-remove-poison-ivy-virus/>.

"The Nitro Attacks: Stealing Secrets from the Chemical Industry." Symantic Security Response, n.d. Web. 26 July 2013. <http://www.symantec.com/content/en/us/enterprise/media/security\_response/whitepapers/the\_nitro\_attacks.pdf>.

"Smithsonian.com." *Smithsonian Magazine*. N.p., n.d. Web. 26 July 2013. <http://www.smithsonianmag.com/science-nature/Top-Ten-Most-Destructive-Computer-Viruses.html>.