Applying an Ethical Framework to this current issue:

Malware uses Facebook and LinkedIn images to hijack your PC

Rhea Mae Edwards

Instructions

1. **For each page, synthesize your research and write in complete sentences in essay format using 14pt type.**
   a. Write about topics/questions provided in the **Notes** below each page.
   b. Add additional pages if you need more room.
   c. If an area doesn't seem to fit your topic, then broaden your research to include similar issues.
      i. When in doubt, write the instructor for clarification using the Canvas Inbox.
   d. Cite sources by using hyperlinks in the Titles of the Article and Titles of Laws. See the examples on the Writing Requirements page.

2. **Add at least one image that provides additional information:**
   a. Chart, illustration, example, infographic, movie (not logos or generic photos).
   b. Cite media with copyright statements: © year Owner Name.
   c. Hyperlink the copyright statement so we can view to the movie in a new tab. (Google PDF files do not allow viewing of the movie.)

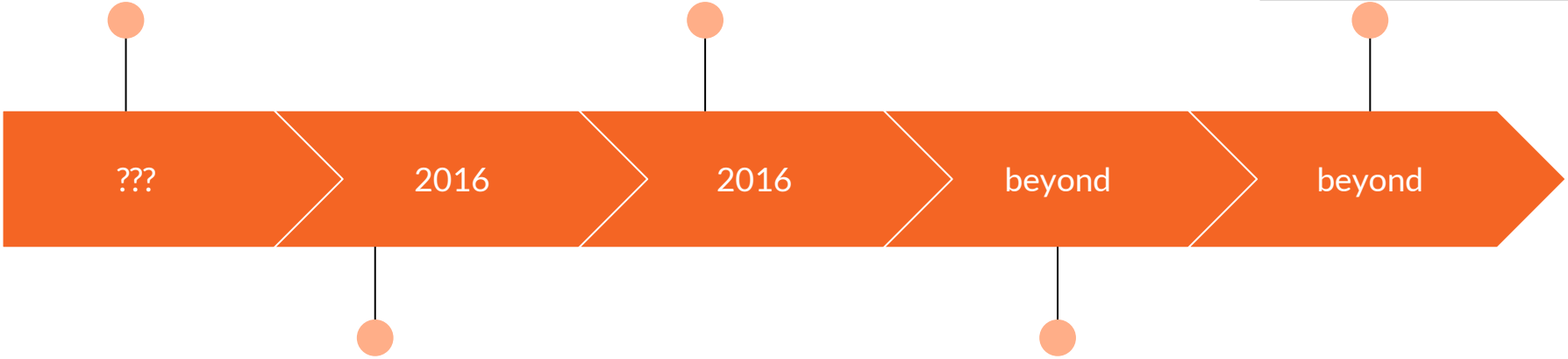
3. **Add all sources to the Bibliography page.**
   a. Include author, title, publisher, date, and URL.

Historical Timeline

Individuals' PCs are being hijacked by voluntarily selecting image links through their Facebook and LinkedIn accounts.

Later stated by Facebook spokesperson reported by the article "Malware uses Facebook and LinkedIn images to hijack your PC", these hijackers were simulated through the additions of bad Chrome extensions scamming individuals, which such extensions are now being blocked by Facebook.

???



Such Malware behavior is being reported by individuals and then to the knowledge of the general public due to many reports being made, such as through the article published by engadget titled "Malware uses Facebook and LinkedIn images to hijack your PC".

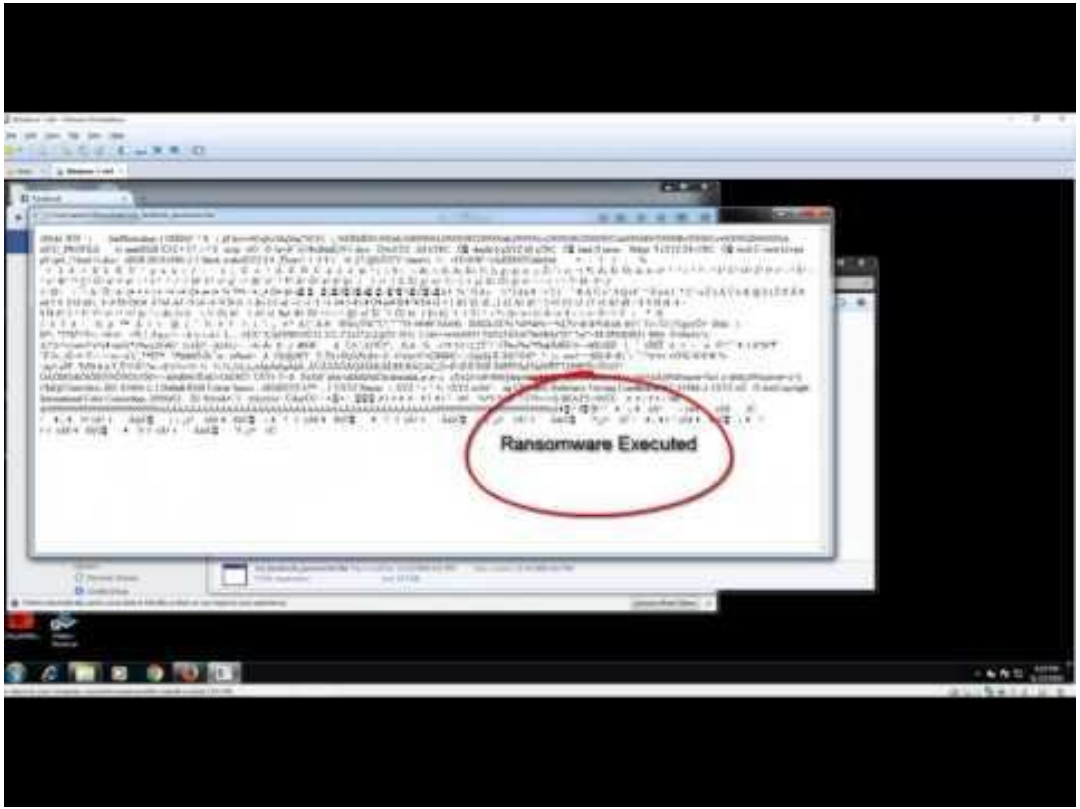
???

Facts of the situation

Due to the unlawful use of malware through the social media networks Facebook and LinkedIn, individuals are unknowingly being technically violated, which is information that I discovered by reading the article “Locky ransomware uses decoy image files to ambush Facebook, LinkedIn accounts” by Tom Mendelsohn. It is reported that linked are selected within these social media platforms, a type of tainted program is download onto the PC in use. This program then hunts down files or certain text documents in order to corrupt. The information inputted within the file or document is then encrypted to where the information displayed is no longer understandable to its original owner. And then the only way to decrypt such nonsense to reclaim important information, is to directly pay the price asked for by the attacker.

In the end, it is a way for individuals to illegal scam and obtain money from others online.

Illustration



Related laws

Unknown

Obligations

Later is it reported to Ars Technica UK updated later in the article “Locky ransomware uses decoy image files to ambush Facebook, LinkedIn accounts”, that Facebook has taken the effort to block such applications through the use of their website, whereas LinkedIn has not reported to use of any further effort.

Apply Ethical Framework 1

Ethical Framework #1: Act Utilitarianism

By using the videos on the course modules page I discovered that...

Apply Ethical Framework 2

Ethical Framework #2: Rule Utilitarianism

By using the videos on the course modules page I discovered that...

The Future

Overall, even though technical techniques, methods, and algorithms will continue to improve and become more complex as we move into the future, such sneaky and also highly knowledgeable individuals will think up and create ways around the system of network security in the technical world. But network security engineers can do their best to prevent intolerable and devastating events to occur by being one step ahead or further of unlawful minds.

To help prevent the use of malware software encrypting others' PCs information, is the continual development and complexity of security software that is programmed onto one's personal computer as the future progresses. By doing so, a hijacker's ability to corrupts one's personal information becomes more difficult to complete. Network security engineers are the type of the people who focus on accomplishing such a task. They have the skill set and knowledge to develop and implement security software into computer systems that will increase the protection of a piece of advanced hardware.

Technology is continually growing and is becoming more complex over time. So it is important to constantly improve the security software that is used by computers such as one's PC, to sufficiently protect such systems from unwanted behavior that is produced and monitored by individuals whose morals may not majorly agree with the ethics that is practiced among the technical society of computer networking.

Bibliography

[1] J. Fingas, "Malware uses Facebook and LinkedIn images to hijack your PC (updated)," in Aol Tech, Engadget, 2016. [Online]. Available: https://www.engadget.com/2016/11/27/ransomware-exploits-facebook-and-linkedin-images/. Accessed: Jan. 19, 2017.

[2] T. Mendelsohn, "Locky ransomware uses decoy image files to ambush Facebook, LinkedIn accounts," Ars Technica UK, 2016. [Online]. Available: http://arstechnica.co.uk/security/2016/11/locky-ransomware-decoy-image-files-boobytrap-facebook-linkdin/. Accessed: Jan. 19, 2017.

[3] Check Point Software Technologies, Ltd., "ImageGate," in YouTube, YouTube, 2016. [Online]. Available: https://www.youtube.com/watch?v=sGlrLFo43pY. Accessed: Jan. 19, 2017.

Citation Style: IEEE