**Mid Term Paper**

**Case Study : Analyzing Stuxnet**

**Value: 150 points**

You may use the document attached to the assignment or download the file from the source.

Read the article titled, “How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History” located at the Wired link below:

<http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1>

Write a six to eight (6-8) page paper in which you:

1. Explain the forensic technique Symantec researchers employed in order to receive the traffic sent by Stuxnet-infected computers and describe what their analysis uncovered.
2. Identify what researchers were surprised to discover with Stuxnet’s malicious DLL file. Assess this significant function of malware and what potential dangers it could present in the future.
3. Determine the primary reason that critical infrastructures are open to attacks which did not seem possible just a couple of decades earlier.
4. Decide whether or not an appropriate case has been made in which Stuxnet was indeed a targeted attack on an Iranian nuclear facility, based on the evidence and conclusions of the researchers. Provide your rationale with your response.
5. Use at least two (2) quality resources in this assignment other than the article linked above. **Note:** Wikipedia and similar Websites do not qualify as quality resources.

Grading for this assignment will be based on answer quality, logic / organization of the paper, and language and writing skills, using the following rubric.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Points: 150** | **Case Study : Analyzing Stuxnet** | | | |
| **Criteria** | **Unacceptable**  **Below 70% F** | **Fair**  **70-79% C** | **Proficient**  **80-89% B** | **Exemplary**  **90-100% A** |
| 1. Explain the forensic technique Symantec researchers employed in order to receive the traffic sent by Stuxnet-infected computers and describe what their analysis uncovered.  Weight: 15% | Did not submit or incompletely explained the forensic technique Symantec researchers employed in order to receive the traffic sent by Stuxnet-infected computers; did not submit or incompletely described what their analysis uncovered. | Partially explained the forensic technique Symantec researchers employed in order to receive the traffic sent by Stuxnet-infected computers; partially described what their analysis uncovered. | Satisfactorily explained the forensic technique Symantec researchers employed in order to receive the traffic sent by Stuxnet-infected computers; satisfactorily described what their analysis uncovered. | Thoroughly explained the forensic technique Symantec researchers employed in order to receive the traffic sent by Stuxnet-infected computers; thoroughly described what their analysis uncovered. |
| 2. Identify what researchers were surprised to discover with Stuxnet’s malicious DLL file. Assess this significant function of malware and what potential dangers it could present in the future.  Weight: 25% | Did not submit or incompletely identified what researchers were surprised to discover with Stuxnet’s malicious DLL file; did not submit or incompletely assessed this significant function of malware and what potential dangers it could present in the future. | Partially identified what researchers were surprised to discover with Stuxnet’s malicious DLL file; partially assessed this significant function of malware and what potential dangers it could present in the future. | Satisfactorily identified what researchers were surprised to discover with Stuxnet’s malicious DLL file; satisfactorily assessed this significant function of malware and what potential dangers it could present in the future. | Thoroughly identified what researchers were surprised to discover with Stuxnet’s malicious DLL file; thoroughly assessed this significant function of malware and what potential dangers it could present in the future. |
| 3. Determine the primary reason that critical infrastructures are open to attacks which did not seem possible just a couple of decades earlier.  Weight: 20% | Did not submit or incompletely determined the primary reason that critical infrastructures are open to attacks which did not seem possible just a couple of decades earlier. | Partially determined the primary reason that critical infrastructures are open to attacks which did not seem possible just a couple of decades earlier. | Satisfactorily determined the primary reason that critical infrastructures are open to attacks which did not seem possible just a couple of decades earlier. | Thoroughly determined the primary reason that critical infrastructures are open to attacks which did not seem possible just a couple of decades earlier. |
| 4. Decide whether or not an appropriate case has been made in which Stuxnet was indeed a targeted attack on an Iranian nuclear facility, based on the evidence and conclusions of the researchers. Provide your rationale with your response.  Weight: 25% | Did not submit or incompletely decided whether or not an appropriate case has been made in which Stuxnet was indeed a targeted attack on an Iranian nuclear facility, based on the evidence and conclusions of the researchers; did not submit or incompletely provided your rationale with your response. | Partially decided whether or not an appropriate case has been made in which Stuxnet was indeed a targeted attack on an Iranian nuclear facility, based on the evidence and conclusions of the researchers; partially provided your rationale with your response. | Satisfactorily decided whether or not an appropriate case has been made in which Stuxnet was indeed a targeted attack on an Iranian nuclear facility, based on the evidence and conclusions of the researchers; satisfactorily provided your rationale with your response. | Thoroughly decided whether or not an appropriate case has been made in which Stuxnet was indeed a targeted attack on an Iranian nuclear facility, based on the evidence and conclusions of the researchers; thoroughly provided your rationale with your response. |
| 5. 2 references  Weight: 5% | No references provided | Does not meet the required number of references; some or all references poor quality choices. | Meets number of required references; all references high quality choices. | Exceeds number of required references; all references high quality choices. |
| 6. Clarity, writing mechanics, and formatting requirements  Weight: 10% | More than 6 errors present | 5-6 errors present | 3-4 errors present | 0-2 errors present |