Activity 1.2.1: Historic Malware - Teacher's Instructions

Malware has existed since the early 1980s and has evolved over the years. Certain malware can be called "historic" because of its unique impact at the time it was released. It could be because it was the first to use a method or because of the harm it caused or because we had to change our computing habits to avoid it. Sometimes it is a personal story about the malware's creator or about the response of law enforcement.

NOTE #1: This project is about getting the students to tell the story of their assigned malware. This accomplishes several goals:

- we are able to cover instruction on a larger number of malware without using instructor lecture.
- students obtain a vocabulary of historic malware so they will have a context when they see references to one in text or articles.
- each student achieves ownership of one historic malware and is motivated to learn that story in depth.
- students grasp the larger picture of how malware has evolved and how society has reacted.

NOTE #2: The 21 listed malware were selected because they each specifically have a good story that is well documented. The resource column indicates which of the required sources has content for that malware. Additional links are provided in cases where there is very good content from an extra source.

NOTE #3: If you have more than 21 students in class, it is recommended that some students double-up on one of the malware marked with an * for which there are resources with extra details. If you have less than 21 students, the 10 most important malware are marked in **bold**.

Lesson Timeline:

DAY 1 - PPT: Malicious Code Attacks Pt1

DAY 2 - Distribute Project Instructions and Malware Template documents. Review instructions and assign students malware from the list. Students begin research.

DAY 3 - Students continue research to complete their Malware summary document.

DAY 4 - Distribute a Malware Notes Sheet to each student for them to write on during presentations. Put students at tables in groups of 4. Give them 6 minutes for all group members to share (appprox 1.5 minutes each) some of the interesting things about their malware, while the others should take notes in their Malware notes sheet. After the 6 minutes students switch to a group with all new people and do it again. With a class of 20 students there will be 4 rotations and students will have notes from at least 10 different malwares.

½ DAY 5 - Use 20 minutes for closure discussion as a whole class. Put the list of malware on the board and offer the following questions:

- Which malware infected the most computers?
- Which malware cost the most?
- Who got in the most/least trouble?
- Which malware came from US government?
- Which malware attacks were accidental or jokes?
- What was something interesting you found out about some malware?

ASSIGNMENT

You have been assigned a historic malware. Research and create a summary document (use Malware Template) that can be used to present to the class in small groups (speed rotation style). You will be expected to hear the presentation of at least 10 others and keep notes on the provided Malware Notes Sheet.

You must include the answers to Questions 1 -4 but for some malware the answers to Q #5 and #6 are not known. I encourage you to include other information of interest about your malware but keep it succinct.

Hand in a summary document/template that INCLUDES the URLs to your research sources. You must have at least 4 sources that meet the requirements list.

Historic Cybersecurity Event Questions

1. What was the malicious action?
2. How did it work?
3. What was the damage?
4. How was it stopped? (What is the defense against it?)
5. Do we know who was involved?
6. Did they get punished?

Requirements for Sources:

- 1 from a state or federal government website (Teacher note: cisa.gov has fact sheets about many of the modern malware in this list).
- 2 from this list:
  - DarknetDiaries.com podcast (DD)
  - Wired.com (W)
  - ArsTechnica.com (A)
  - KrebsOnSecurity.com (K)
  - WeLiveSecurity.com (WL)
- 1 from any website

SEARCH TIP: You can use the Google "site" operator to specify a search within a certain site or type of domain. Examples:

site: *.gov "Melissa virus"

site: wired.com "Slammer worm"

Resources - indicates which of the required sources has known content for that malware. See ReferenceArticles.zip for articles for student sharing.	**Student Name**	**Malware**
W – WL – video		**Morris Worm 1988** - Video resource
W – WL		Melissa Virus 1999
W – WL		I Love You Virus 2000 (aka Love Letter Virus)
W – A		Code Red Worm 2001
W – A - WL		**Slammer Worm 2003** (aka Warhol worm)

W – A		MyDoom 2004
W – A - WL		Sasser / Netsky 2004
W – A - DND #61		Sammy 2005
K - W – A - WL		Zeus 2009
K - W – A - WL - extra article		**Conficker 2009**
K - Wired article - A - WL - DND #29		**Stuxnet 2010**
K - W – A - WL		Flame 2012
W – A - WL		**GameOver Zeus 2014**
K - W – A - WL		CryptoLocker 2015
K – A		NanoCore RAT 2015
K - W – A - WL- extra article		**Mirai Botnet 2016**
K - Wired article - A - WL - DND #73		**WannaCry Ransomware 2017**
K - Wired article - A - WL - DND #54		**NotPetya 2018** (Ukraine shutdown)
K - W – A - WL		**Emotet Trojan 2018**
K - W – A		RobbinHood Ransomware 2019 (Baltimore/Atlanta)
K - W – A - WL		**Trickbot 2020**

GRADING RUBRIC - Research & Present Historic Malware

Project Part	REQUIREMENTS	Grade
Summary Document	· Student name · Name of assigned malware · URLs for at least 4 different online resources - see requirements above · Written narrative (not bullet points) on malware info - min 3 paragraphs · No spelling or grammar errors	20
Presentation	· Share information about your malware in an interesting and comprehensive way · Able to answer questions for more details · Make eye contact with audience and speak clearly · Listen and pay attention while others are presenting	5
Note Sheet	· You are to listen to at least 10 presentations and write down at least 2 things about each. You will turn in the note sheet at the end.	10
TOTAL		35