Activity 1.2.1: Historic Malware - Student 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.

In the list below 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 Questions 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**

Resource Abbreviations:

- DarknetDiaries.com (DND)
- Wired.com (W)
- ArsTechnica.com (A)
- KrebsOnSecurity.com (K)
- WeLiveSecurity.com (WL)

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