**Outline**

·         This is an individual assignment.

·         You will be assigned one of the following virus topics.

·         Research your topic to learn about computer malware and to prepare a presentation about your topic.

·         Suggested Slide Topics and layout for your presentation is provided below.

·         The presentation should be between 5-10 minutes and will be given in front of the class.

·         Slides should be shared with Mr. Nestor (p0079141@pdsb.net) via. Google drive.

**Virus Topics**

1.   CIH Virus – 1998

2.   Melissa Worm – 1999

3.   Code Red Worm – 2001

4.   Slammer Worm – 2003

5.   SoBig.F Worm – 2003

6.   My Doom Worm – 2004

7.   Stuxnet Worm – 2010

8.   Cryptolocker Trojan – 2013

9.   ZeroAccess Botnet – 2013

10.  Superfish Adware – 2014

11.  Locky Ransomware – 2016

12.  WannaCry Ransomware - 2017

How locky works is by sending an email to a victim. The victim will then open the email, and download the attached word document or excel file. Inside the file is a bunch of gibberish, with instruction to enable embedded macros to make it human readable. If the victim does enable the macros, their computer will be infected with malicious code as the virus hides in the macros the victim released. The gibberish from earlier than will rescramble itself to be a message which tell the victim about their fate, and holds their files hostage and asks them to pay a ransom ranging from 0.5 to 1 bitcoin.

**Suggested Slide Layout**

1.   Overview

·         Summarize what is known about the malware

·         Provide: Year / Creator / Origin

·         Its classification: Virus / Worm / Trojan / DoS Attack / Email Phish, etc.

Locky is a type of ransom ware released in 2016 by a group of highly skilled hackers.

2.   Any Other Interesting Facts

·         This will be topic dependent

It uses social engineering to infect Windows PCs, comes with powerful features to disguise itself, and can encrypt more than 160 types of files, including source code and databases. Locky’s behavior and found it uses various scripting languages for delivery. It has advanced features such as domain generation algorithm, complex spam email campaigns, server-side encryption, and generic PE packers. Since its release, its authors have fine-tuned it and added features to make Locky even more difficult to detect. Keys are generated on the server side, making manual decryption impossible, and Locky ransomware can encrypt files on all fixed drives, removable drives, network and RAM disk drives. Payment varies between 0.5 and 1 bitcoin.

3.   Its Targets

·         Target Hardware Type: e.g. PC, Network, Smartphone, etc.

·         Target Operating System: e.g. Windows, Mac, Android, etc.

·         Target Software Applications

On release in February 2016, there were no known pattern between victims of the ransomware

But in its second debut in May 2016 its victims has specified to Amazon users

The second iteration affected and estimated 30 - 100 million Amazon Users

As time went on, locky had become more advanced

Newer version of locky started to appear in June and July, but made its third big appearance in August as it started to attack the healthcare industry

When locky in installed onto a person's computer it can:

4.   What it Did

·         What it did to Computer Hardware

·         What it did to Computer Software

·         What it did to Computer Data

Encrypt a large amount of data stored on the computer

If possible upload itself to servers to further spread the virus (only possible on the more advanced versions)

Inform victims about their misfortune

Demand ransom in the form of bitcoin

5.   How it Worked

·         How did it get into a computer

Via an email.

·         How did it spread between computers

The hacker group responsible for locky has used advanced bot programs which were made to be undetectable and send email messages to to victims

The victims would receive an email for varying reasons depending on which iteration of the ransomware is released

The email would contain a microsoft word document, or another application which would prompt the reader to enable macros in order to view the document’s contents

Recipients who enable the macros would instead end up downloading and installing the ransomware

OR would the virus would be sent through a zip file which when opened automatically executes the virus

6.   Its Effect

·         Summarize its Financial impact

·         Summarize its User Base impact

No exact numbers have been released on the damages caused by the ransomware

But due to the estimated millions of users it has affected, one can assume at least several million files have been encrypted and lost forever

As well as potential thousands of bitcoin without any confirmation to if the victims got their files back or not

7.   Its Control

·         How was it discovered

·         How was it stopped

·         How can it be removed

Due it being a ransomware, its own nature reveals itself

In order to deal with the virus, victims had to ge their devices scanned by their their antiviruses to delete and malicious files installed

Unfortunately, they could recover encrypted files

Beyond that, the only way to protect themselves from the virus was to be wary of all emails they received, especially those which had contained some type of downloadable file attacked

8.   Sources

* “Amazon Users Targets of Massive Locky Spear-Phishing Campaign.” *Threatpost English Global Threatpostcom*, threatpost.com/amazon-users-targets-of-massive-locky-spear-phishing-campaign/118323/.
* KnowBe4. “Locky Ransomware.” *KnowBe4*, www.knowbe4.com/locky-ransomware.
* “Locky Ransomware – What It Is and How to Protect Your PC.” *Avast*, [www.avast.com/c-locky](http://www.avast.com/c-locky).

Resources

<https://www.symantec.com/connect/blogs/bios-threat-showing-again>

<https://www.symantec.com/security-center/writeup/2000-122113-1425-99>

<https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/zeroaccess-indepth-13-en.pdf>

Resources

<https://www.symantec.com/connect/blogs/bios-threat-showing-again>

<https://www.symantec.com/security-center/writeup/2000-122113-1425-99>

<https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/zeroaccess-indepth-13-en.pdf>