Clarence V. Kimbrell Jr.

CYSE 280 – Windows Systems Management and Security

Professor Malik A. Gladden

Homework 7

1. What are the benefits of folder and file auditing?

The largest benefit to folder and file auditing is the extra layer of security. It allows for a file-sharing environment without putting critical folders or files in the wrong hands.

2. What are the advantages and disadvantages of using Microsoft Encrypting File System to protect files and folders?

EFS works within a workgroup or active directory domain environment and encrypts files from authorized access. So, it provides yet another layer of security. One of the disadvantages is that the information can be lost during operating system reinstallation.

3. What are the main characteristics of XML Paper Specification (XPS)?

The main characteristics of XPS are that documents are stored in a print spooler using the appropriate format which is XP. Secondly, the document is converted to XPS format and then rendered.

4. What are the advantages of using a Separator Page?

You can determine if the printer is in improper spooling format. Also, it is great for sectioning off parts of a longer document.

5. What is ZeuS and how does it work?

ZeuS is malware posed as a double-edge threat. It was used to steal banking information and then turn the computer into a spy that was completely operated remotely. Lastly, the computer with ZeuS was added to a botnet.

6. How did law enforcement agencies and security researchers attempt to take down ZeuS?

Security researchers join in to help Microsoft's Digital Crime Unit take down the botnet by attacking its command-and-control servers and the domains involved.

7. What were some of the challenges in combating ZeuS?

One of the biggest challenges was that the central system was hosted in a place that was not reachable. Then it had to be a coordinated takedown which required thousands of domains to be reported and analyzed. This created a longer investigation because ZeuS was very resilient.

Sources:

https://www.elcomsoft.com/WP/advantages_and_disadvantages_of_efs_and_effective_recovery_of_encrypted_data_en.pdf

https://darknetdiaries.com/transcript/111/