Module 5 & 6, and

Darknet Diaries, Episode # 111: ZeuS

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 280 - Windows Systems Management and Security, Professor Malik A. Gladden

July 03, 2025

Short Answer Questions: Short answers should typically be three to four sentences long. It is crucial to be concise while providing a thorough response. Alternatively, you have the option to upload a two-minute audio or video recording to answer the questions.

Module 5 & 6

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

Folder and file auditing allows administrators to track access to sensitive data, helping detect unauthorized access or potential insider threats. Auditing helps government departments and organizations meet internal and external compliance metrics, including data protection regulations, by maintaining accurate access logs. Auditing can also assist in forensic investigations by revealing who accessed or modified files and when they did so. Thus, auditing improves both security visibility and accountability.

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

Advantages include seamless integration with Windows, transparent encryption, and user-level access control without requiring third-party tools. However, **disadvantages** include dependency on user profiles—if the encryption certificate/key or account access is lost, then the data becomes inaccessible. Also, EFS does not protect data in transit or prevent deletion, and it's not effective against all malware or privileged user attacks. Lastly, EFS also relies on the strength of user passwords, and weak credentials can undermine its security.

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

XML Paper Specification (XPS) is a fixed-layout document format developed by Microsoft that preserves document fidelity across different platforms and printers. It uses XML to describe the layout, appearance, and printing information of a document. XPS is similar in function to PDF, supporting vector graphics, text, and embedded fonts for accurate rendering. The format aims to maintain consistency regardless of the software or hardware used to view it. XPS files typically have the .xps or .oxps file extension.

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

A Separator Page can help organize print jobs by clearly dividing documents from different users or tasks. It may include useful metadata, such as username, date, or file name. That improves efficiency in shared printing environments and reduces the chance of print jobs getting mixed up. It also helps in auditing and tracking print usage. Separator pages are better suited for large institutions or companies that have print devices capable of handling a high volume of print jobs rather than small businesses or small offices that perform much lower volumes of print jobs.

Listen to "Episode #111: ZeuS of the DarkNet Diaries podcast which can be found at https://darknetdiaries.com/episode/111Links to an external site.
Based on the podcast, answer the following questions.

5. What is ZeuS, and how does it work?

ZeuS is a sophisticated banking Trojan malware that infected millions of computers, allowing thieves to steal financial credentials. Afterward, the operators of ZeuS would use the login credentials to gain access to online bank accounts and transfer money from them to offshore accounts. It worked by logging keystrokes, capturing login credentials, and manipulating web browsers to intercept banking transactions. The malware spreads through phishing emails or drive-by downloads, often remaining undetected while siphoning funds via money mules. Over time, the creator of ZeuS added many new and dangerous features. One feature included a botnet system that would silently infect machines, enabling attackers to control and carry out large-scale financial fraud remotely.

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

Global law enforcement agencies (e.g., the FBI) and cybersecurity researchers collaborated to identify the infrastructure and actors behind ZeuS (e.g., Operation Tovar). They analyzed command-and-control servers, developed sinkholes to disrupt botnet traffic, seized botnet infrastructure, employed digital forensics to trace perpetrators, and collaborated with Major Tech companies and banks to freeze fraudulent accounts and transactions (e.g., Microsoft)—these efforts aimed to dismantle the malware's network and trace its creators, like the coder Slavik.

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

First, combating ZeuS was difficult due to its decentralized peer-to-peer architecture, frequent code obfuscation, and the use of bulletproof hosting and server redundancy. Second, the malware constantly evolved; the variant evolutions of ZeuS, like Gameover ZeuS, outpaced early detection efforts. Third, someone leaked the source code to the public, allowing other criminals to modify and reuse it. Fourth, legal barriers across jurisdictions also hampered coordinated law enforcement efforts against the globally distributed actors. The malware's operators were based in Russia and had a history of harboring and tolerating state-sponsored cybercriminals who targeted Russia's enemies.