Infection Detection of Emotet Malware Using Capture-Display-Analyze Model in Wireshark Packet Extraction

Te-Min Liu,
Network Traffic Packets Analysis Association,Taiwan
En-Chun Kuo,
Da-Yu Kao,
Central Police University, Taiwan

Abstract

- The paper presents a lightweight Capture-Display-Analyze (CDA) model for an instant packet extraction to capture packets, display filters, and analyze symptoms from a local network interface.
- This lightweight CDA model introduces an efficient packet extraction algorithm to find interesting connections, observe network symptoms, and reveal their behavior patterns at a microscopic level.

I. Introduction

- The worm-like features of an Emotet banking malware result in rapidly spreading network-wide infection.
- Its initial infection occurs when users open the macro malware document through emails.
- It can evade typical signature-based detection and generate false indicators in a virtual environment.
- Cybercrime investigators in Law Enforcement Agencies (LEAs) have been using Wireshark to monitor network traffic, develop a clear perspective of activity, conduct deep packet inspection, and generate insights into real-time or historical packets across the network.

II. Proposed CDA Model for Instant Packet Extraction Procedure

1 Capture Filters: View Filtered Packets While Capturing

- ☐ Check the Network Connection Status (Netstat)
- ☐ Identify the Background Network Traffic (Wireshark)
- ☐ Filter the Internet Background Noise or Broadcast Packets (Filter)
- ☐ Recheck Online Network Status

2 Display Filters: Display Filtered Packets While Viewing

- ☐ Unsolicited Domain Name Query (“dns” or “udp.port==53”)
- ☐ Unsolicited Website Query (“http” or “tcp.port==80”)
- ☐ Unsolicited File Transfer Query (“ftp” or “tcp.port==21”)
- ☐ Unsolicited Execution File Query
- ☐ Filter Background Network Noise

3 Analyze Symptoms: Analyze Colour Coding

- ☐ Static Signature
- ☐ Dynamic Analysis
- ☐ Network Analysis

III. Conclusions

The study provides a lightweight client-side method with a high detection rate to discover the network behavior patterns, reveal the network symptoms, and minimize the damage brought by a macro virus.

Acknowledgment

This research was partially supported by the Executive Yuan of the Republic of China under the Grants Forward-looking Infrastructure Development Program (Digital Infrastructure Information Security Project-109).