Inside Cridex – Memory Analysis Case Study

memoryforensic.com/inside-cridex-memory-analysis-case-study/

Husam Shbib 2 October 2024

Introduction

Cridex, also known as Dridex, is a banking worm (evolved over the year to be full-featured banking malware) that employs advanced techniques to evade detection and facilitate the theft of financial information. Memory forensics is crucial in analyzing Cridex due to its ability to operate in memory and evade traditional file-based detection methods.

Keep in mind that this study case is not a full walk-through investigation, instead, it gives you just an idea on analyzing memory dumps. It will be beneficial, especially for beginners to get started.

As MemoryForensic is a collaborative blue team platform, we are sharing valuable community-contributed resources like this one – Cridex case study.

Note: Fileless malware or memory-resident malware don’t necessarily mean that all stages of the cyber kill chain occur entirely in memory. While certain steps, such as execution and command-and-control communication, may happen in memory, other stages like initial infection, persistence mechanisms, or lateral movement might involve writing to disk, using registry keys, or dropping small files as triggers.

Credit

This work is done by Diyar Saadi, and this article is based on his work and analysis.

Downloading the Cridex Memory Dump / Running on the Cloud Lab

> Attention: the sample you are about to download may include malicious files and malware samples. To protect your system, please analyze it on a completely isolated virtual machine if it is not running on cloud

You can download the memory dump directly from here.

Used Tools

- Volatility2
- **Volatility WorkBench**2
- VirusTotal

Cridex Analysis Steps

- Using Volatility:
  - Load the memory dump into a forensics tool like Volatility.
  - Use plugins to extract information about running processes, network sockets, and loaded DLLs.
- Identifying Malicious Processes:
  - Look for processes that exhibit suspicious behavior, such as unusual names or those running from unexpected locations.
  - Check for injected code or modified processes that may indicate Cridex activity.
- Checking Network Connections:
  - Analyze active network connections to identify communications with known Cridex command and control servers.
  - Use the netscan or connscan plugins to identify any abnormal network activity.
- Recovering Artifacts:
  - Extract artifacts like clipboard content, which might contain stolen information, or passwords saved in memory.
  - Use the cmdscan or consoles plugins to examine command history that might reveal user interactions with the malware.
- Detecting Persistence Mechanisms:
  - Analyze the registry keys and services that might indicate how Cridex maintains persistence on the infected system.
  - Look for unusual entries that may have been created by the malware.

The Case Study Document

Cridex-Malware-Memory-AnalysisDownload

Conclusion

We briefly analyzed Cridex malware residing in a memory dump, provided some tips and tricks, that will give you a start in analyzing memory dumps.

We hope that you download the memory dump in safe environment, try analyzing it before the case study file to better enhance your memory analysis skills.

~ Cya till the next one 🙂