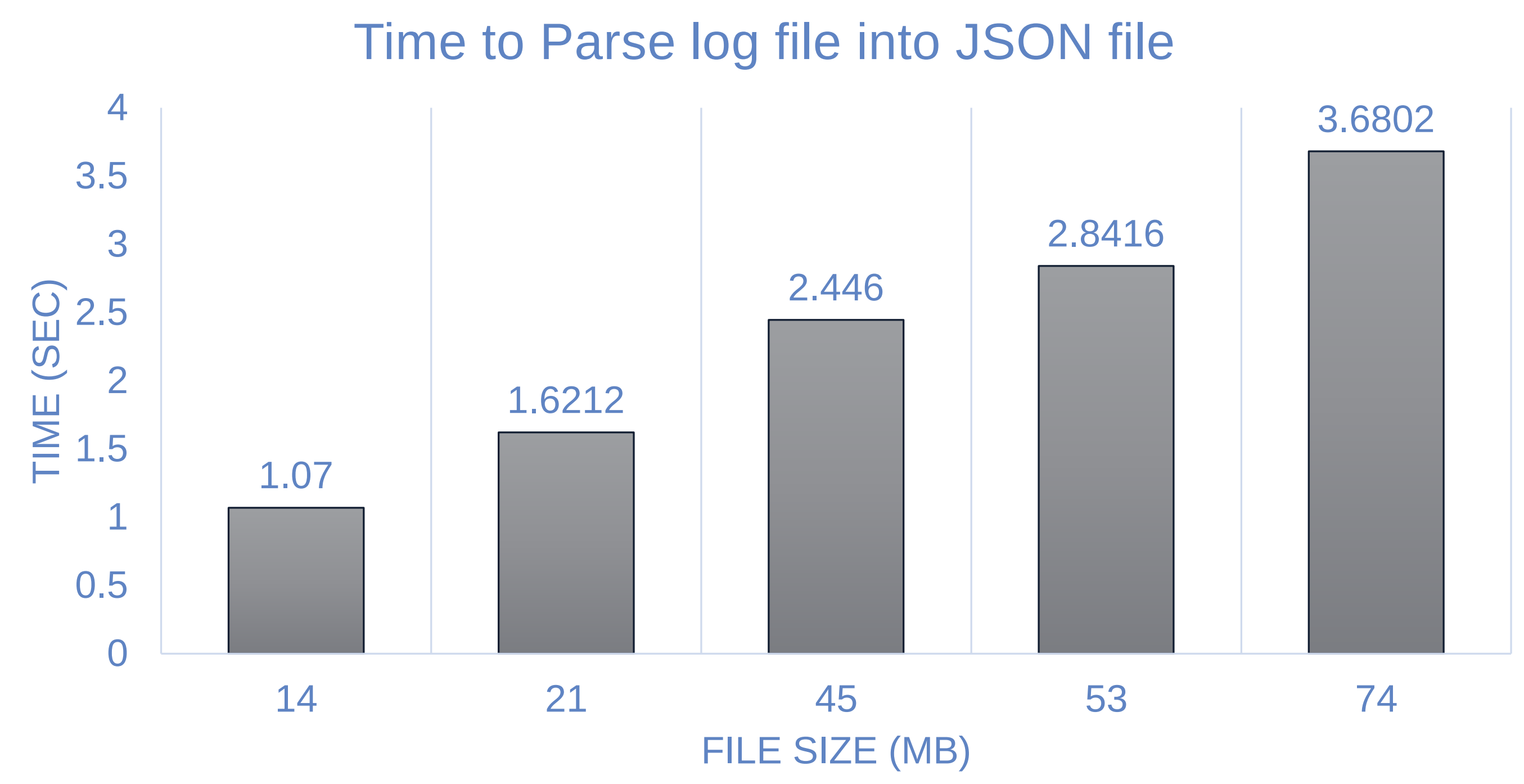
# WinLog: Data Provenance Recording for Windows

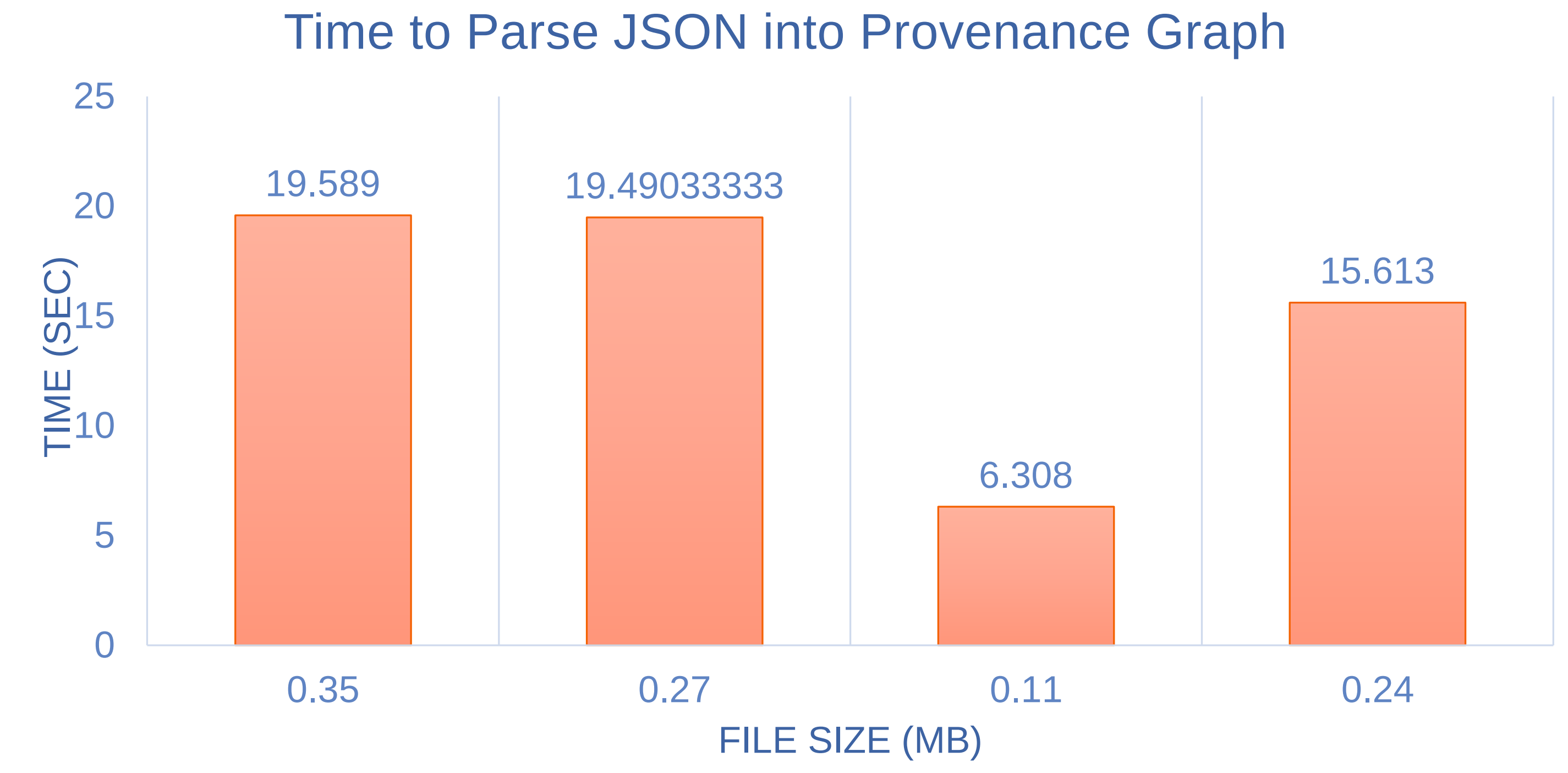
**Muhammed Imran, Meghana Muthekepalli, Wajih Ul Hassan**
Department of Computer Science, University of Illinois at Urbana-Champaign

## INTRODUCTION

- Data Provenance is metadata that describes the lineage of a data object and models system execution as a causal relationship graph.
- It allows forensic investigators to find the root cause and ramifications an attack.
- OS-based provenance trackers such as LPM and Linux Audit produce whole-system provenance.
- However, there is no Windows based provenance tracker.
- We present WinLog a system that seamlessly collects and manages provenance data on Windows OS.
- It generates provenance graphs with all the causal relationships.

## Evaluation





**Source Code can be found at:**
**https://github.com/Wajihulhassan/winprov**

ILLINOIS

PURE
Promoting Undergraduate Research in Engineering

## DESIGN

- WinLog consists of 3 components:
  1. Parser
     - Parses log file into data provenance relationships.
  2. Publisher
     - Sends data provenance in JSON format to MQTT server.
  3. Visualizer
     - Fetches JSON messages from MQTT and generates provenance graphs.

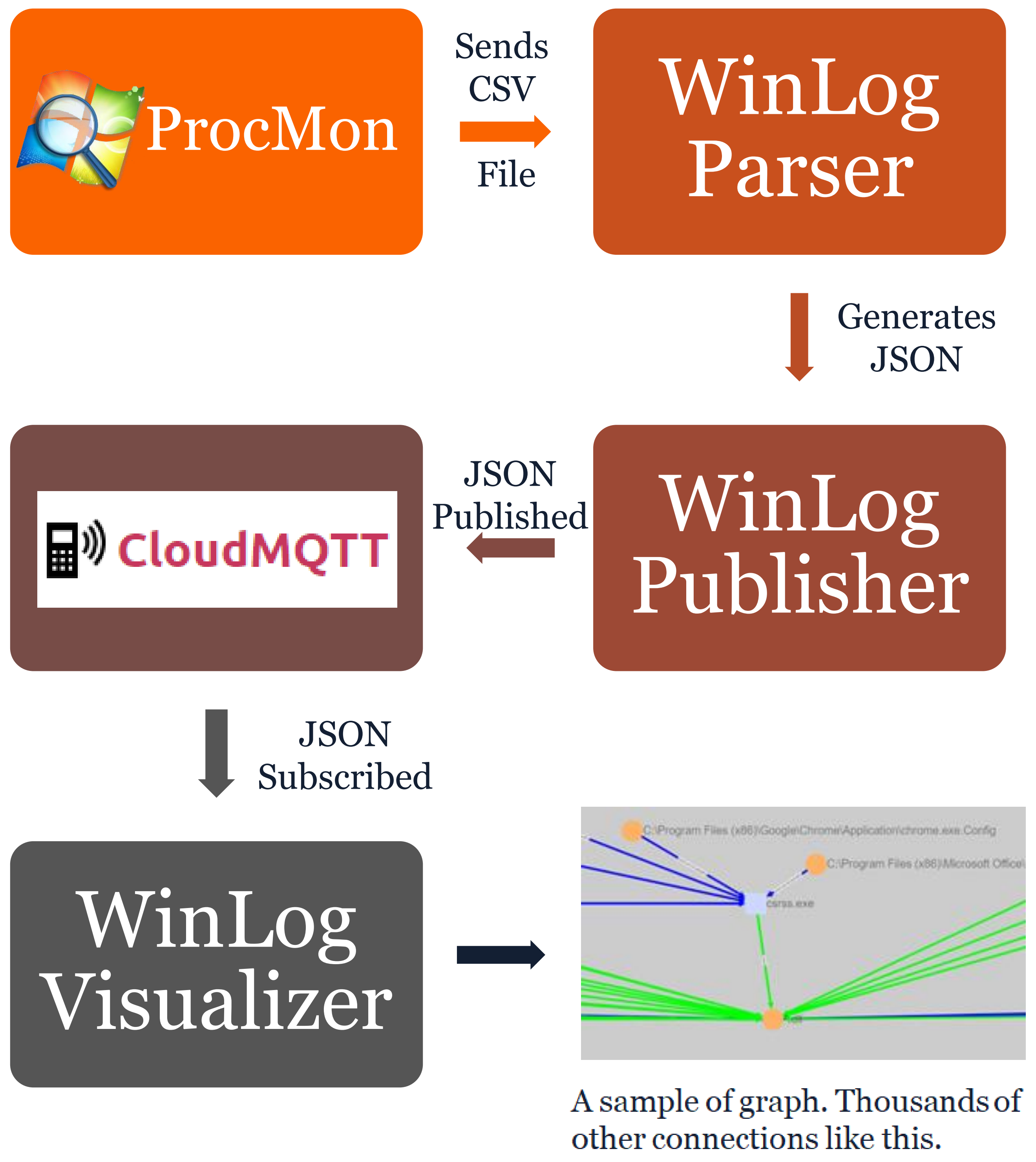

ProcMon
Sends CSV File
WinLog Parser
Generates JSON
WinLog Publisher
JSON Published
CloudMQTT
JSON Subscribed
WinLog Visualizer
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe.Config
C:\Program Files (x86)\Microsoft Office
A sample of graph. Thousands of other connections like this.

*Figure 1: WinLog architecture and workflow*

## Attack Case Study

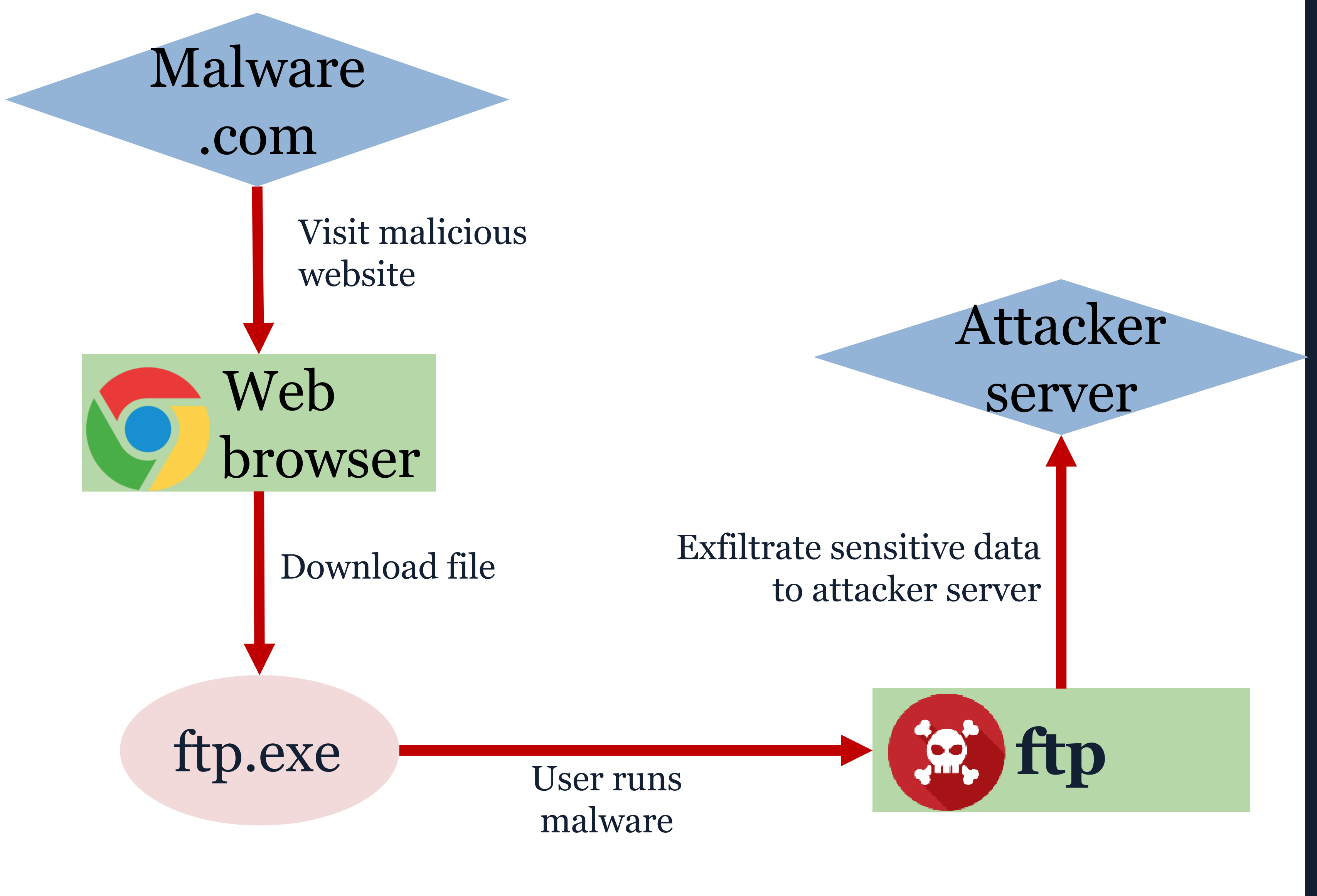


*Figure 2: Malicious software download*