A Visual Analytics based approach on identifying Server Redirections and Data Exfiltration

Introduction

How to better find potential cyberattacks is the billion question facing security researchers and practitioners. In this work, we innovatively designed a graphic based system overview that can make suspicious activities related to server redirection attack and data exfiltration easier to identify.

The Challenge

Need for better overview Design

Must be scalable, accurate, and fast.

Reveal security events rather than plotting data.

Potential "Big" Data

GB to TB in size. 70 million records in our data set.

Interactive Design

Helping investigating suspicious events.

Situation Awareness

Be able to monitor the network system

Our Approach

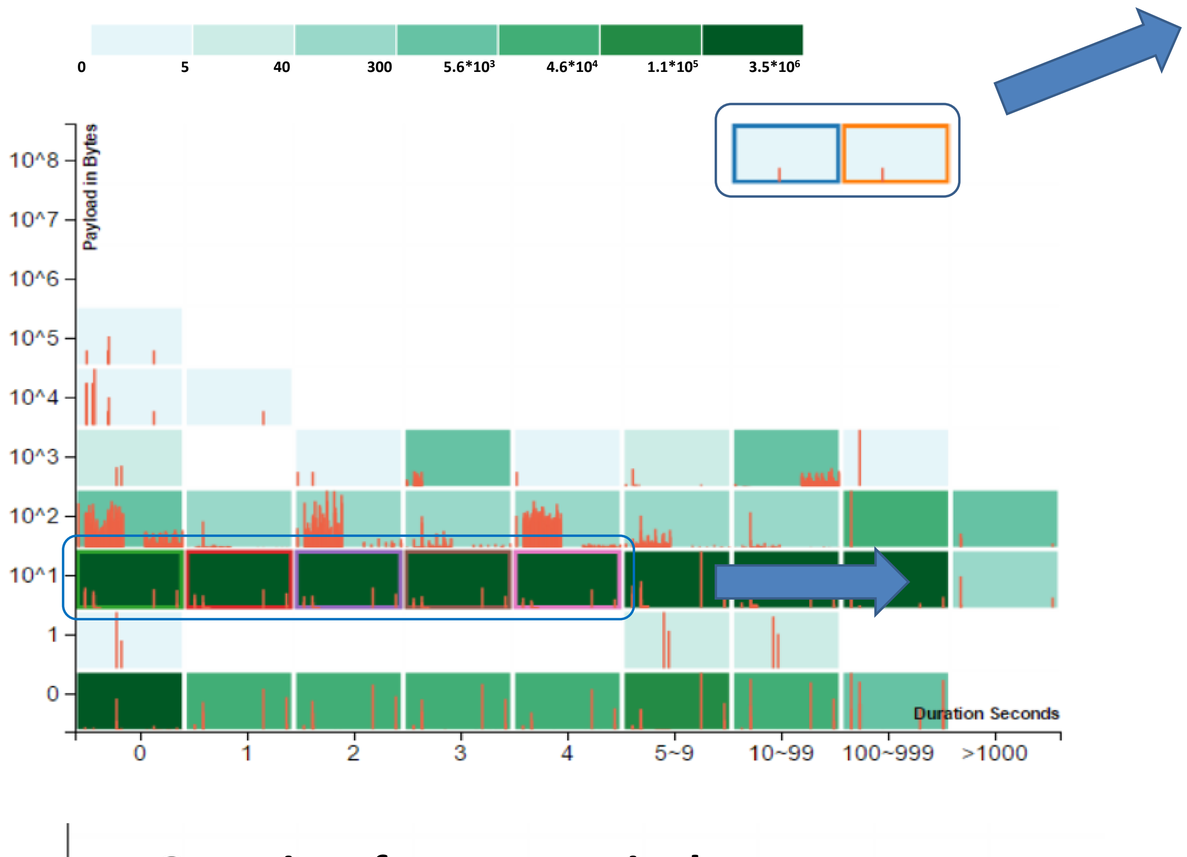
--Visualize aggregated traffic characteristics from network flows.

--Payload and session duration are two key parameters in the overview design.

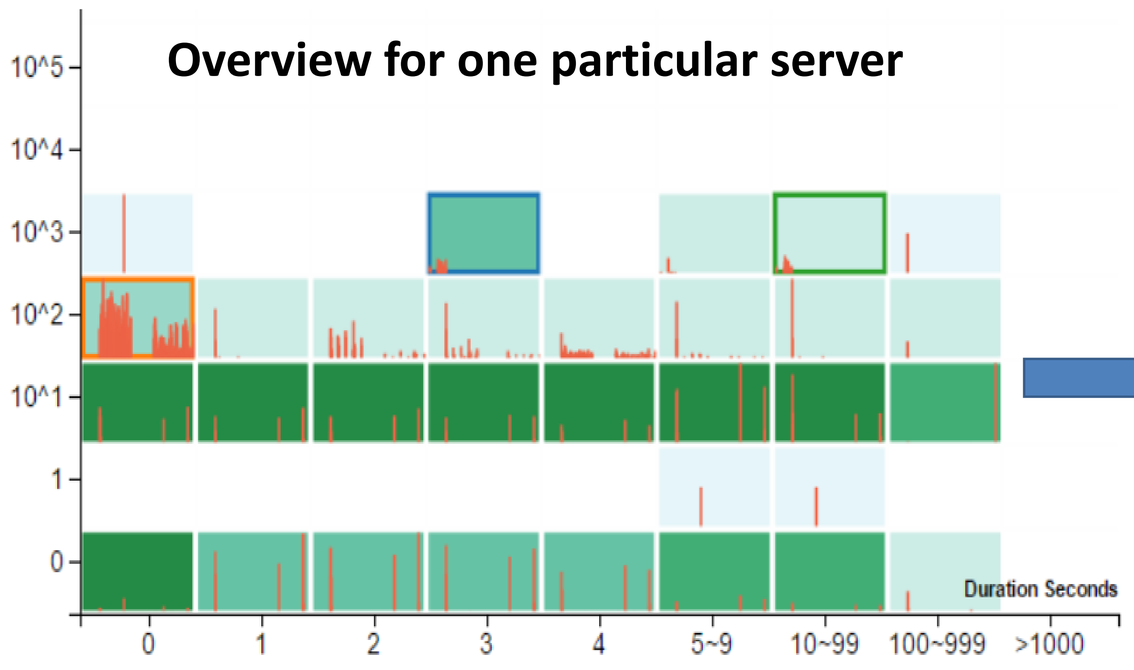
--Multiple cell graphs visualize time-series events in different ranges.

--Web-based application, Node.js, MySQL, and d3.js (visualization library)

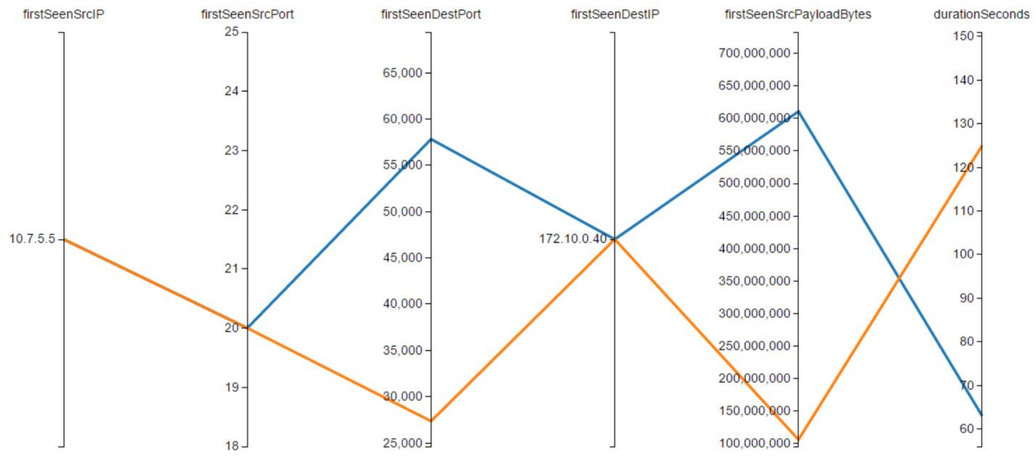
Overview for the network



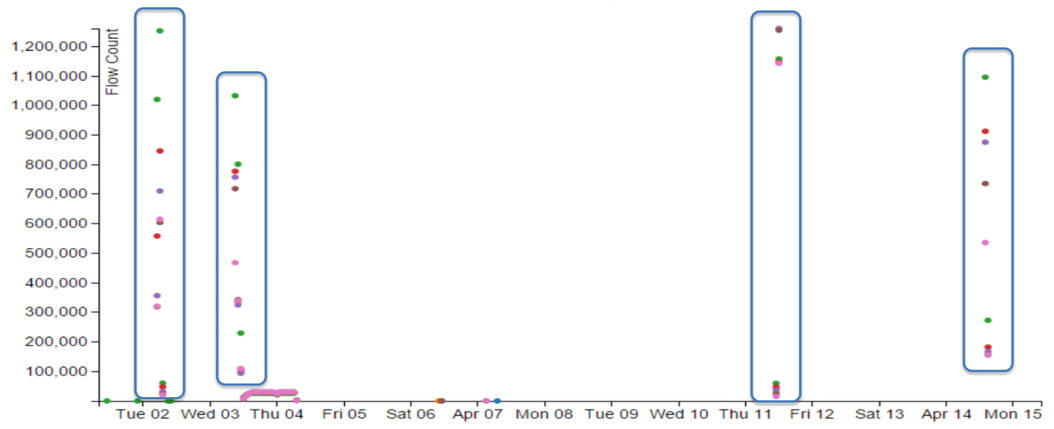
Overview for one particular server



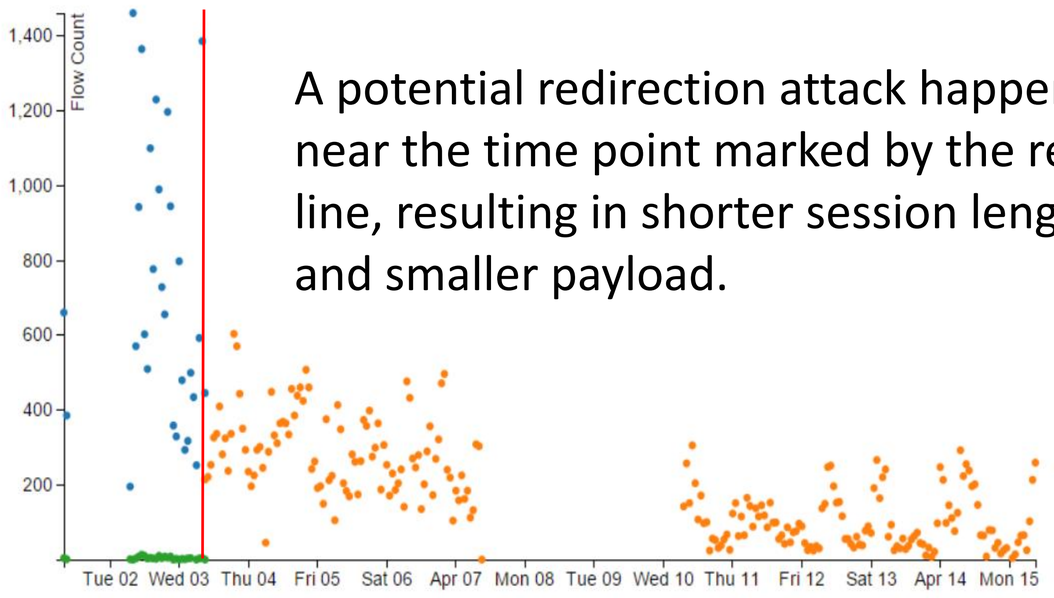
Suspicious netflow pattern shift (from blue and green rectangle to orange rectangle)



These two records indicates potential data exfiltration because of the extremely large payloads.



Further investigation identified these four events are either denial of service attack or port scan attack.



A potential redirection attack happened near the time point marked by the red line, resulting in shorter session length and smaller payload.

Wang, Weijie, CIT
Yang, Baijian, CIT
Chen, Yingjie Victor, CGT