DNS FIREWALL DATA VISUALIZATION

Thursday 11th April, 2019

Stanislav Špaček
Anna-Marie Dombajová, Vít Rusňák

Introduction

Motivation

- Cybersecurity tools produce a large amount of log data
- The log data contain information useful for CSIRT incident handlers to keep situation awareness

Issue

- The log data are generated too fast and in different formats
- Aggregation and visualization need to be specified for the data to be human-readable

Data visualization

- We prototyped the visualization for the DNS Firewall cybersecurity tool
- The visualization is based on the experience of CSIRT incident handlers and Schneiderman's Mantra

Schneiderman's Mantra

1. Overview First
2. Zoom and Filter
3. Details on Demand

CSIRT-MU

Log Data Types

Operational Data

- Generated as the DNS queries hit the DNS FW blacklist
- Analysis may point incident handlers to an infected device

Management Data

- Generated as incident handlers manage the DNS FW
- Allows keeping track of blacklist history

DNS Firewall Data Views

Should answer three key questions:

1. WHO? – the view should aggregate all blocked attempts originating from the same source, so an *IP address* with a large number of accesses within a specified time-frame can be easily singled out.
2. WHERE TO? – the view should aggregate all blocked attempts directed towards the same *Domain*. A *Domain* with a large number of access attempts within a specified time-frame is easy to reveal.
3. WHEN? – the view should aggregate the access attempts with a predefined granularity (e.g., 24 hours).

Prototype Components

Heatmap Calendar

- Shows the distribution of events over time
- Answers the *WHEN?* question

Tables

- Allow for detailed examination of events
- Support filtering and ordering based on displayed parameters

Domain/IP address Inspector

- In the form of a bar chart
- Shows the details from the perspective of a domain or an IP address

Summary

- Visualization of log data generated by cybersecurity tools helps incident handlers keep situation awareness
- The data views need to be customized with the respect to the tool and the anomalies they should highlight
- However, some views may be generalized over similar tools, e.g. different types of firewalls

CSIRT-MU

THANK YOU FOR YOUR ATTENTION

csirt.muni.cz

@csirtmu

Stanislav Špaček

spaceks@ics.muni.cz