



PowerBI Cybersecurity Dashboard

Mayah Bosworth

Company Software Security Analysis Dashboard: Overview

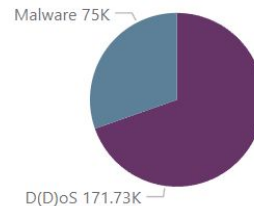
Instances Captured

247K

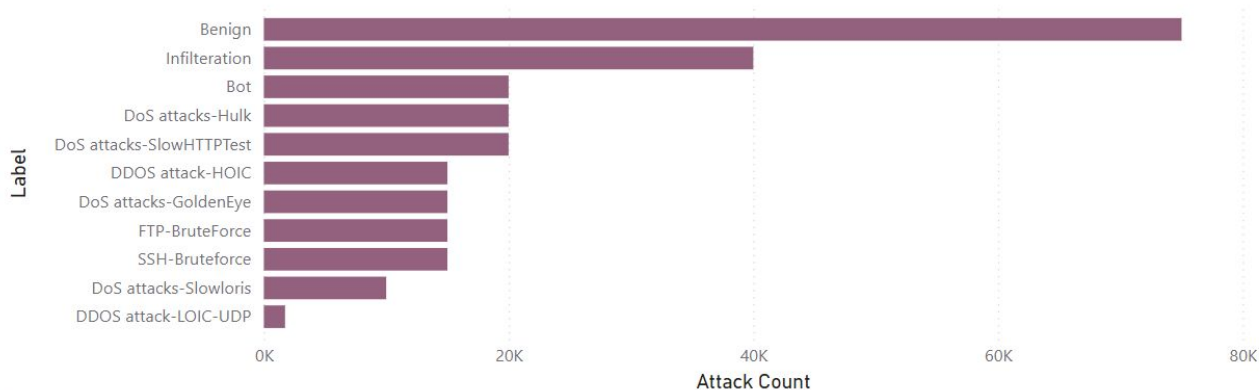
Attack Count by Attack Category



Method of Attack



Attack Count by Label



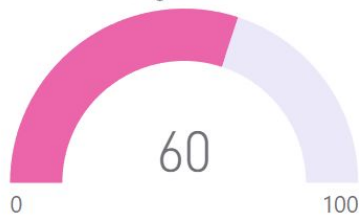
Company Security Analysis: D(D)oS Attacks

Active / Idle Time Detected

No Active / Idle Time Detected

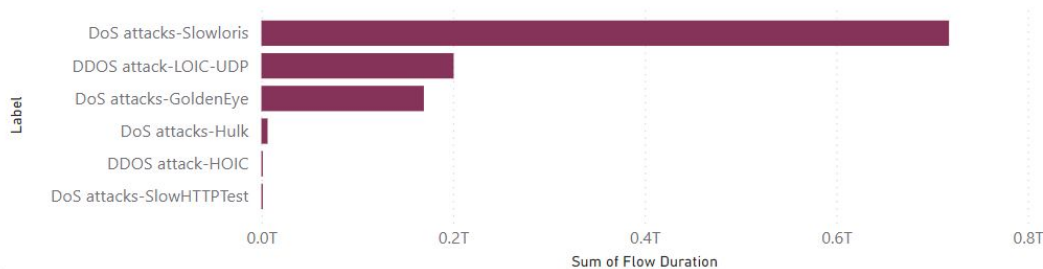
Active / Idle Time Detected

Danger Level

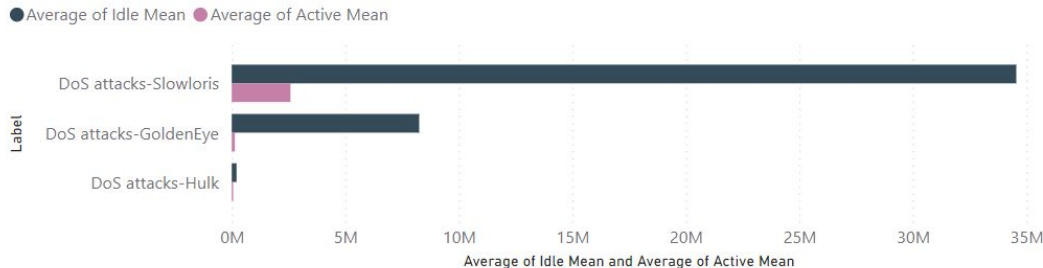


- Disrupt service availability
- Periods of activity and rest (harder to detect)

Sum of Flow Duration by Label (seconds)



Average of Idle Time and Average of Active Time by Label (seconds)



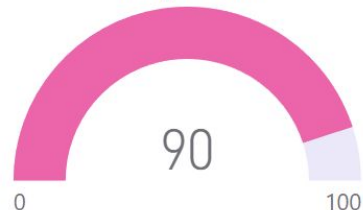
Company Security Analysis: D(D)oS Attacks

Active / Idle Time Detected

No Active / Idle Time Detected

No Active / Idle Time Detected

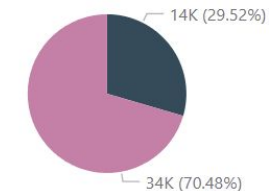
Danger Level



- Prolonged connectivity
- High volume of packets
- Immediate service disruption

Total Bwd Pkts vs Total Fwd Pkts by Label

DDOS attack-HOIC



DoS attacks-SlowHTTPTest



DDOS attack-LOIC-UDP



● Sum of Tot Bwd Pkts
● Sum of Tot Fwd Pkts

DDOS attack-HOIC

48K

Sum of Total Packets

DDOS attack-LOIC-UDP

203M

Sum of Total Packets

DoS attacks-SlowHTTPTest

40K

Sum of Total Packets

Company Security Analysis: Malware

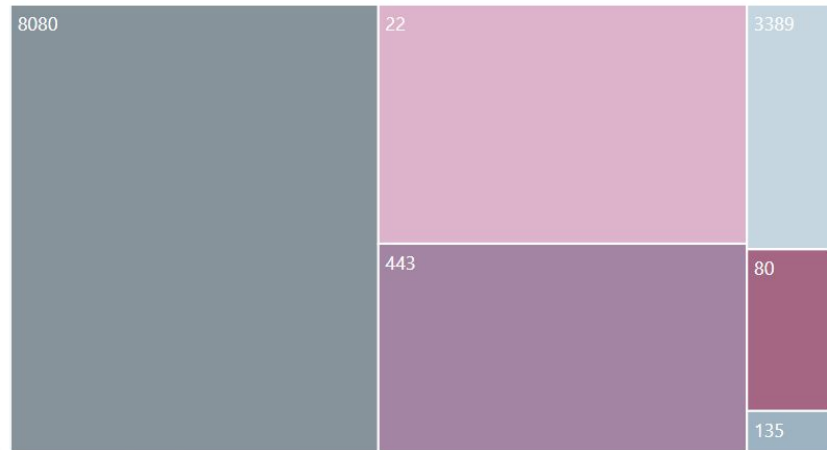
Malware Overall

Malware Overall

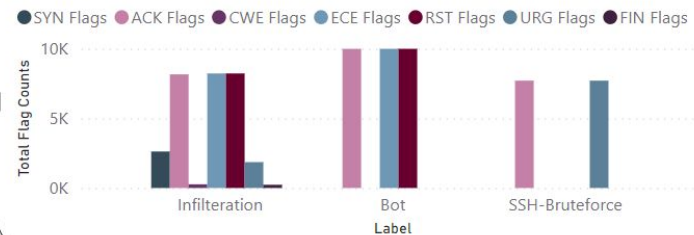
Remote Network & Access Management

Web Traffic

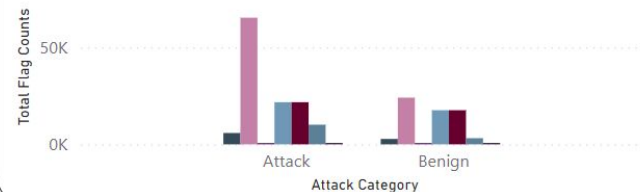
Sum of Total Flags by Destination Port (Top 6)



Malware Indication Total Flag Counts



Flag Counts by Category



Company Security Analysis: Malware

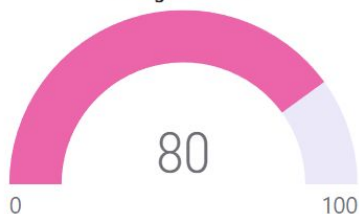
Malware Overall

Web Traffic

Remote Network & Access Management

Web Traffic

Danger Level



Port 80 (HTTP Web Traffic):

- No SYN flags indicate overwhelming existing browser connections

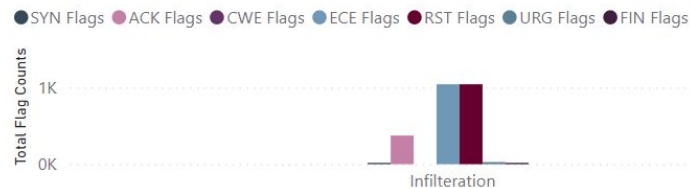
Port 8080 (Alternative HTTP Web Traffic)

- Disruption for dev and/or testing webpages

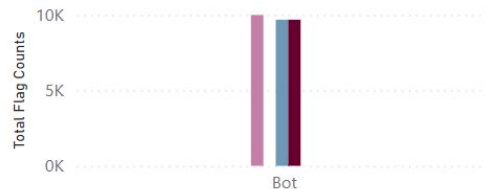
Port 443 (HTTPS Web Traffic):

- SYN and ACK flags indicate successful connections
- Prone to data exploitation

Malware Indication Total Flag Counts: Port 80 (HTTP)



Malware Indication Total Flag Counts: 8080 (Alternative HTTP)



Malware Indication Total Flag Counts: 443 (HTTPS)



Company Security Analysis: Malware

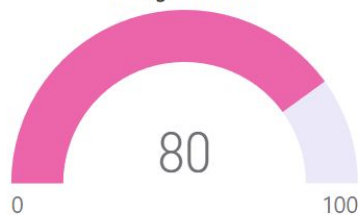
Malware Overall

Remote Network & Access Management

Web Traffic

Remote Network & Access Management

Danger Level



Port 3389 (Remote Desktop Protocol):

- High ECE and RST flags indicate network congestion

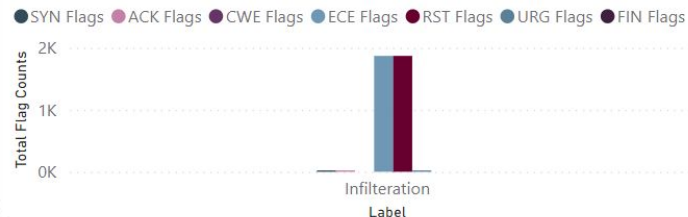
Port 135 (Microsoft Remote Procedure Call)

- No FIN flag indicates no closed connection

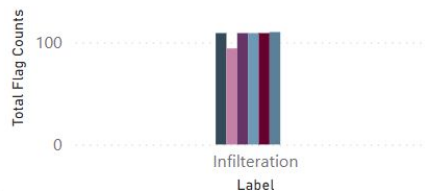
Port 22 (Secure Shell):

- High ACK and URG flags indicate many log in attempts

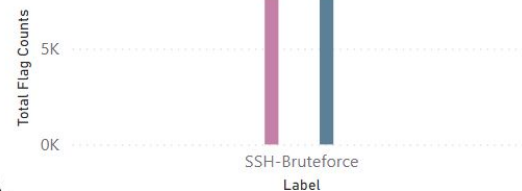
Malware Indication Total Flag Counts: Port 3389 (RDP)



Malware Indication Total Flag Counts: Port 135 (Microsoft RPC)



Malware Indication Total Flag Counts: Port 22 (SSH)



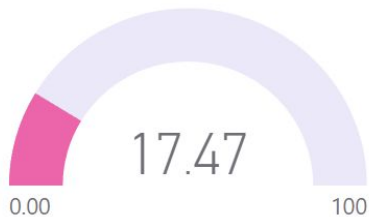
Company Security Analysis: Recommendations and Ideal KPIs

Current Overall Company Danger Ranking



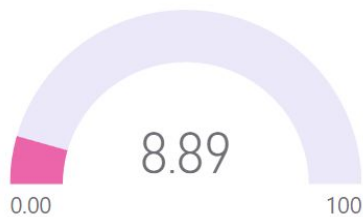
Step 1:
Install Anti-Malware Software

Projected Overall Company Danger Ranking



Step 2:
Install Web Application Firewalls

Projected Overall Company Danger Ranking



Step 3:
Rate Limiting for UDP Floods

Ideal Overall Company Danger Ranking

