SHARING AND AUTOMATION FOR PRIVACY PRESERVING ATTACK NEUTRALIZATION

Demonstration of large-scale endpoint profiling

SAPPAN @ CSIRT-MU

Tomas Jirsik and Michal Pavuk

(Masaryk University)

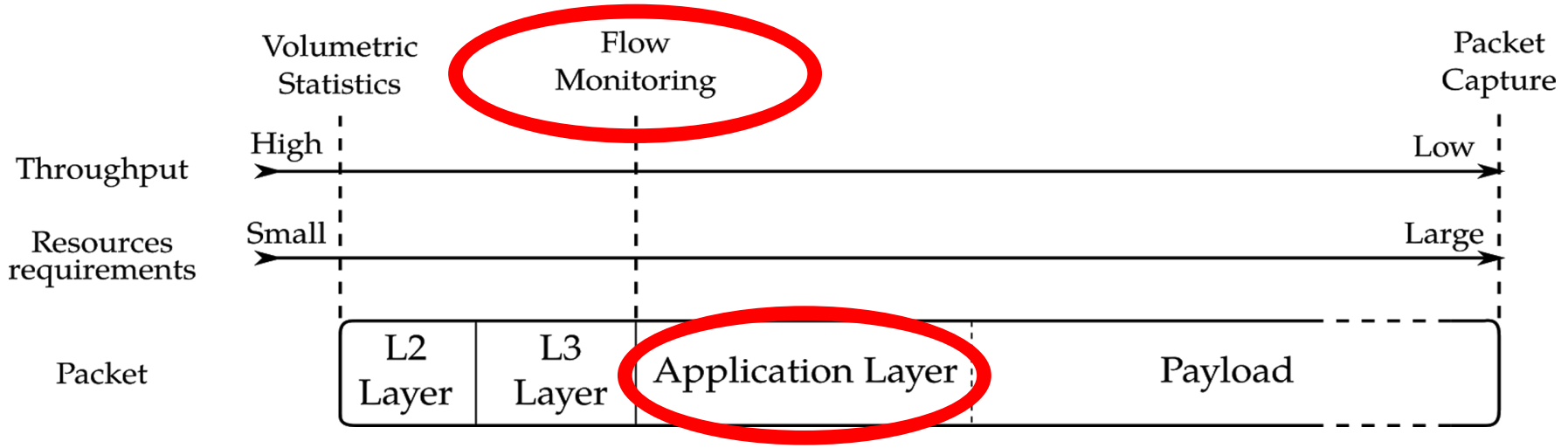
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Agenda

- Data Sources
- Endpoint Profiles
- Sample Use cases
- Visual Exploration of the Profiles

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Data source – Network Telemetry



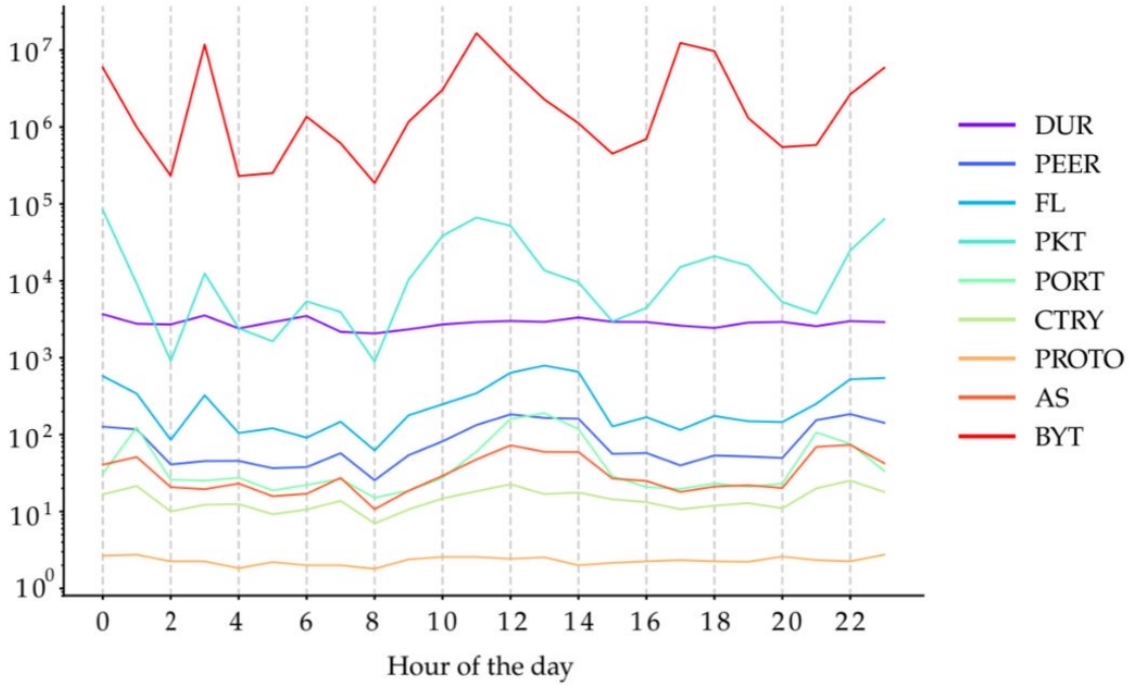

```
Date first seen          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags Tos  Packets    Bytes      pps      bps    Bpp Flows
2020-05-14 23:54:29.556   275.212 TCP      [redacted]:34801 ->      [redacted]:443    ....AP...    0       12      828        0       24     69     1
2020-05-14 23:58:46.186     0.000 UDP      [redacted]:5287  ->      [redacted]:53     ........     0        1      103        0        0    103     1
2020-05-14 23:58:40.989     0.000 UDP      [redacted]:123   ->      [redacted]:49268  ........   184        1       76        0        0     76     1
2020-05-14 23:58:43.425     0.000 UDP      [redacted]:123   ->      [redacted]:50982  ........   184        1       76        0        0     76     1
2020-05-14 23:56:51.713   112.003 ICMP     [redacted]:0     ->      [redacted]:771    ........     0        3      168        0       11     56     1
2020-05-14 23:58:43.107     0.000 UDP      [redacted]:55954 ->      [redacted]:88     ........     0        1      207        0        0    207     1
2020-05-14 23:54:30.349   299.371 TCP      [redacted]:443   ->      [redacted]:49423  ....AP.S.    0       26     3.3 K       0       90    129     1
2020-05-14 23:54:59.748   298.399 TCP      [redacted]:9999  ->      [redacted]:40716  ....AP...    0       85    17.4 K       0      476    209     1
2020-05-14 23:59:58.776     0.000 UDP      [redacted]:54101 ->      [redacted]:53     ........   184        1       97        0        0     97     1
2020-05-14 23:59:59.811     0.000 UDP      [redacted]:42330 ->      [redacted]:53     ........     0        1       67        0        0     67     1
Summary: total flows: 10, total bytes: 22.2 K, total packets: 132, avg bps: 551, avg pps: 0, avg bpp: 172
Time window: 2020-05-14 23:53:49 - 2020-05-15 00:04:59
Total flows processed: 2605, Blocks skipped: 0, Bytes read: 1048505
Sys: 0.082s flows/second: 31559.7    Wall: 0.007s flows/second: 327179.1
```


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Endpoint profile – network telemetry

HOST-RELATED IP FLOW FEATURES

Type	Name	Aggregation
Aggregations	# of flows (FL)	src IP
	# of packets (PKT)	src IP
	# of bytes (BYT)	src IP
	Flow duration (DUR)	src IP
Distinct counts	# of peers (PEER)	src IP, dst IP
	# of ports (PORT)	src IP, dst ports
	# of protocols (PROTO)	src IP, dst ports
	# of AS numbers (AS)	src IP, dst AS number
	# of countries (CTRY)	src IP, dst country



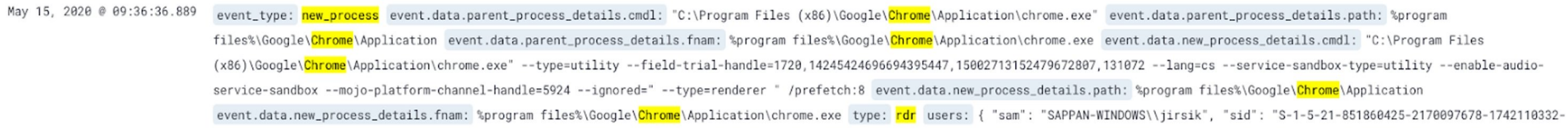
Additional features

- Day/night ratios
- In/Out ratios
- Aggregations over extended time period
- Top N statistics

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Data source – Endpoint Telemetry

- System Logs
- Events by F-Secure
  - new/open/stop process
  - module load
  - create thread
  - registry write
  - file access
  - network connection
  - powershell events
  - OS security events



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Endpoint profile – endpoint telemetry

F-SECURE events

- process tree

Aggregate stats:

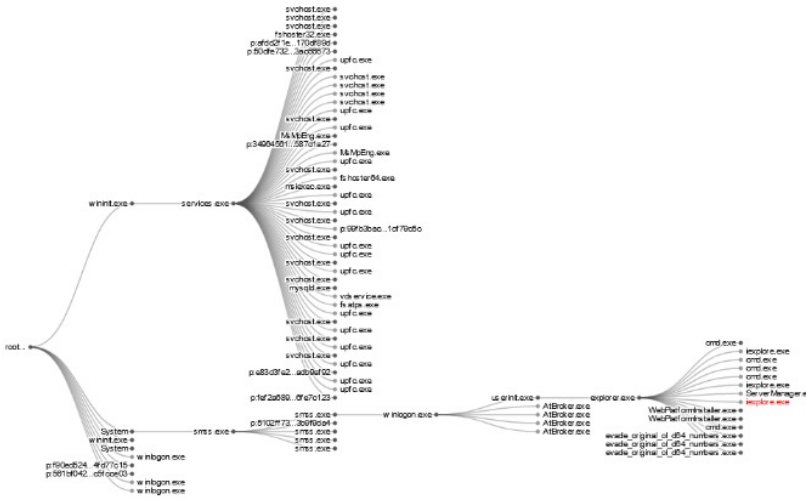
- num_logs -> total number of logs
- num_logons -> num of logs with event ID 4624 (An account was successfully logged on)
- num_dst_tasks -> number of distinct tasks which generated the logs
- num_dst_sources -> number of distinct sources which generated the logs
- num_wsa -> number of events where source is Microsoft-Windows-Security-Auditing

Host OS:

- name -> e.g. Windows 10 Education version build

Top stats:

- tasks: top 5 tasks which generated the most logs
- sources: top 5 sources which generated the most logs



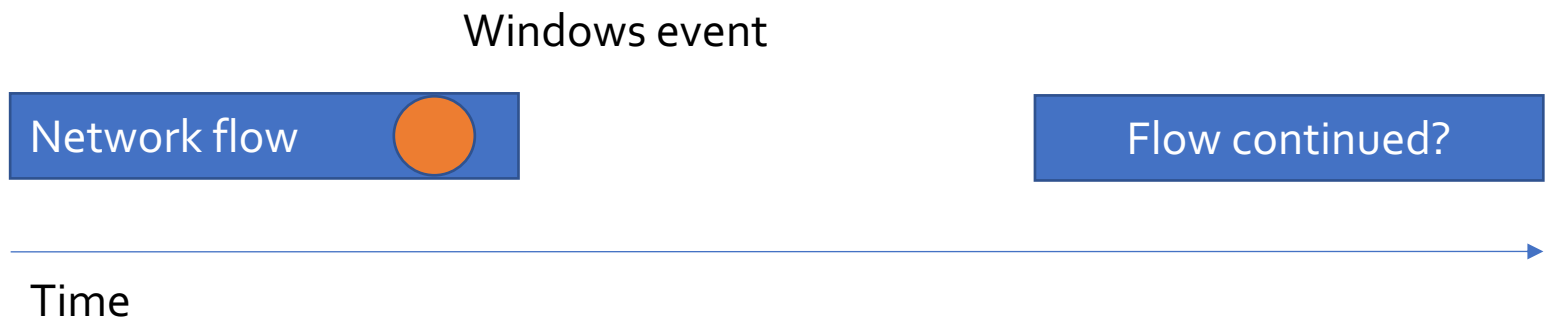
Process

6148	not elevated
GPID:	p:724f3d69017254d91c08bedc682df65b
Name:	iexplore.exe
Path:	%program files%\internet explorer
Command:	"C:\Program Files\internet explorer\iexplore.exe"
User:	SAPPAN-WINDOWS\obrecht
SHA1:	5d5586e4273110d48f2cd8b19a91e8853de5e02c

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Data Correlation

- Based on common attributes
  - Source & Destination IP and ports
  - Sliding time window
- Problems
  - Not all network events are logged
  - Reuse of the source ports by the OS



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

How can be the profiles used?

- **Clustering of profiles**
  - identification of groups with similar properties
  - different purpose
  - segmentation
  - variability (security)
- **Classification**
  - profile assignment
- **Long Term Observations**
  - history of host behaviors
- **Visual Analytics**
  - explorative analysis
  - get understanding

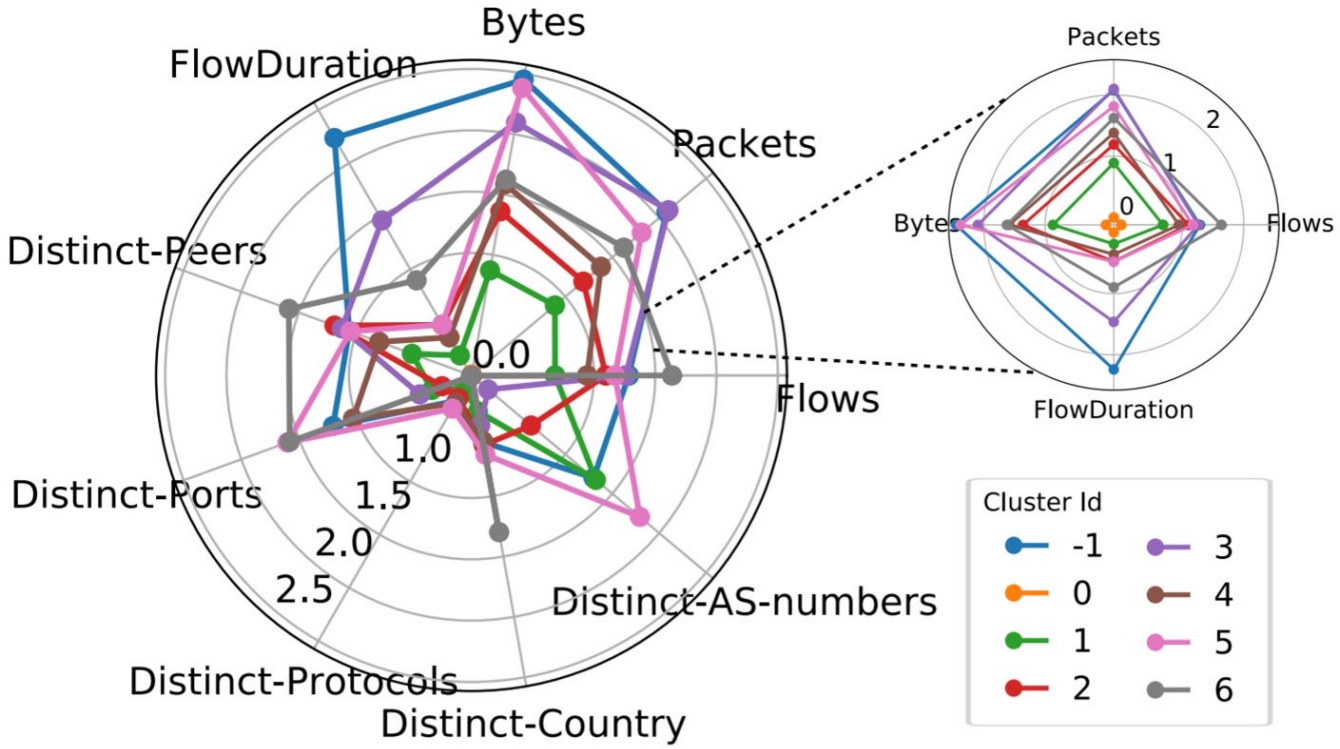


Fig. 9. Representation of clusters of hosts with similar variability of behavior characteristics.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Profile Usecase I

Temporal patterns in behavior

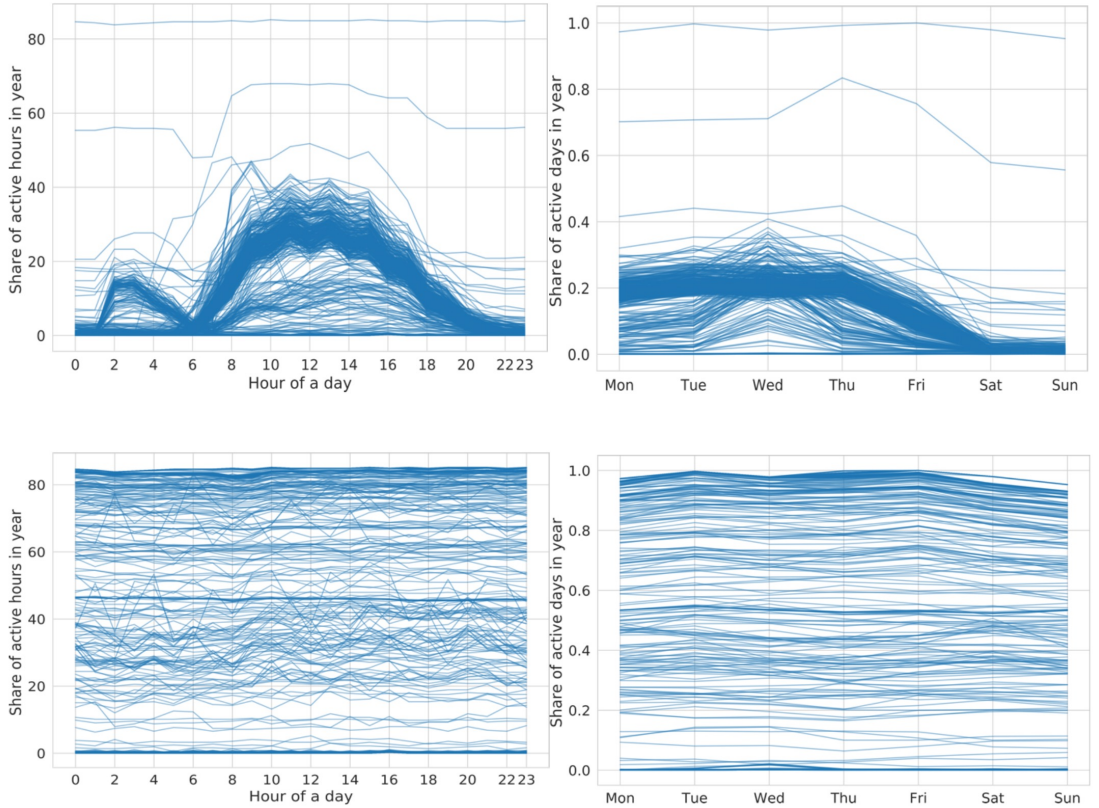
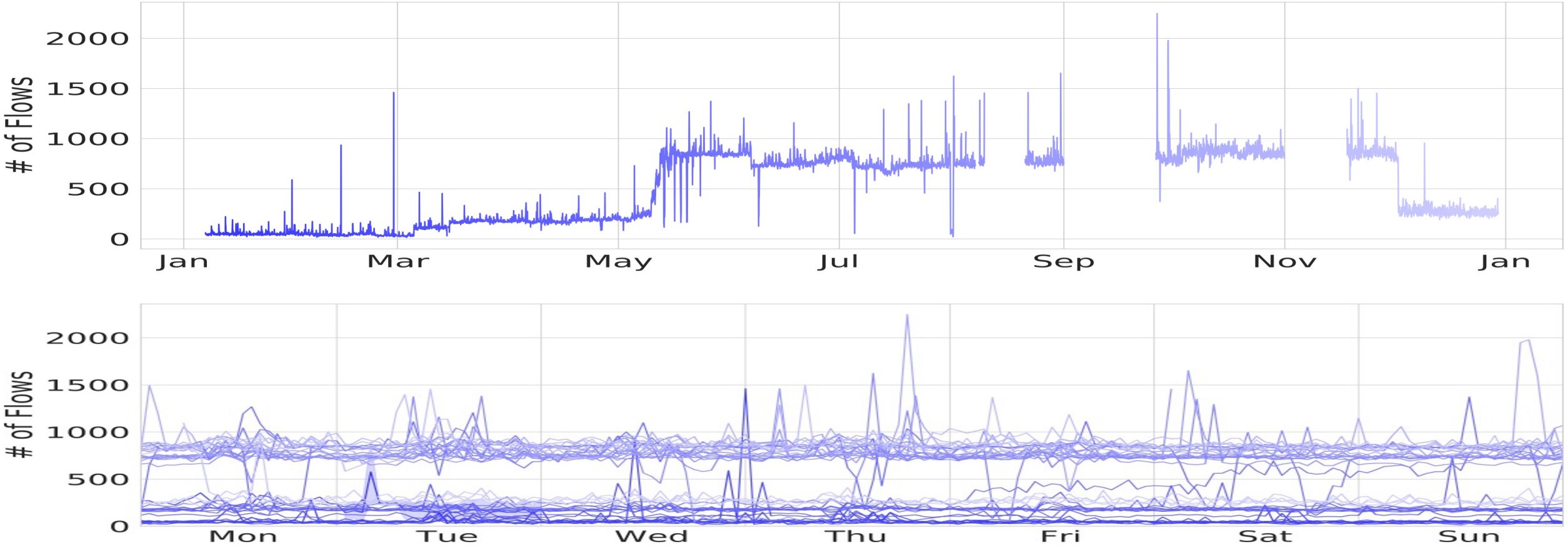


Figure 9:Temporal patterns present in workstation's (above) and server's (below) behavior during a day (left, in %) and week (right, in 0-1)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Profile Usecase II

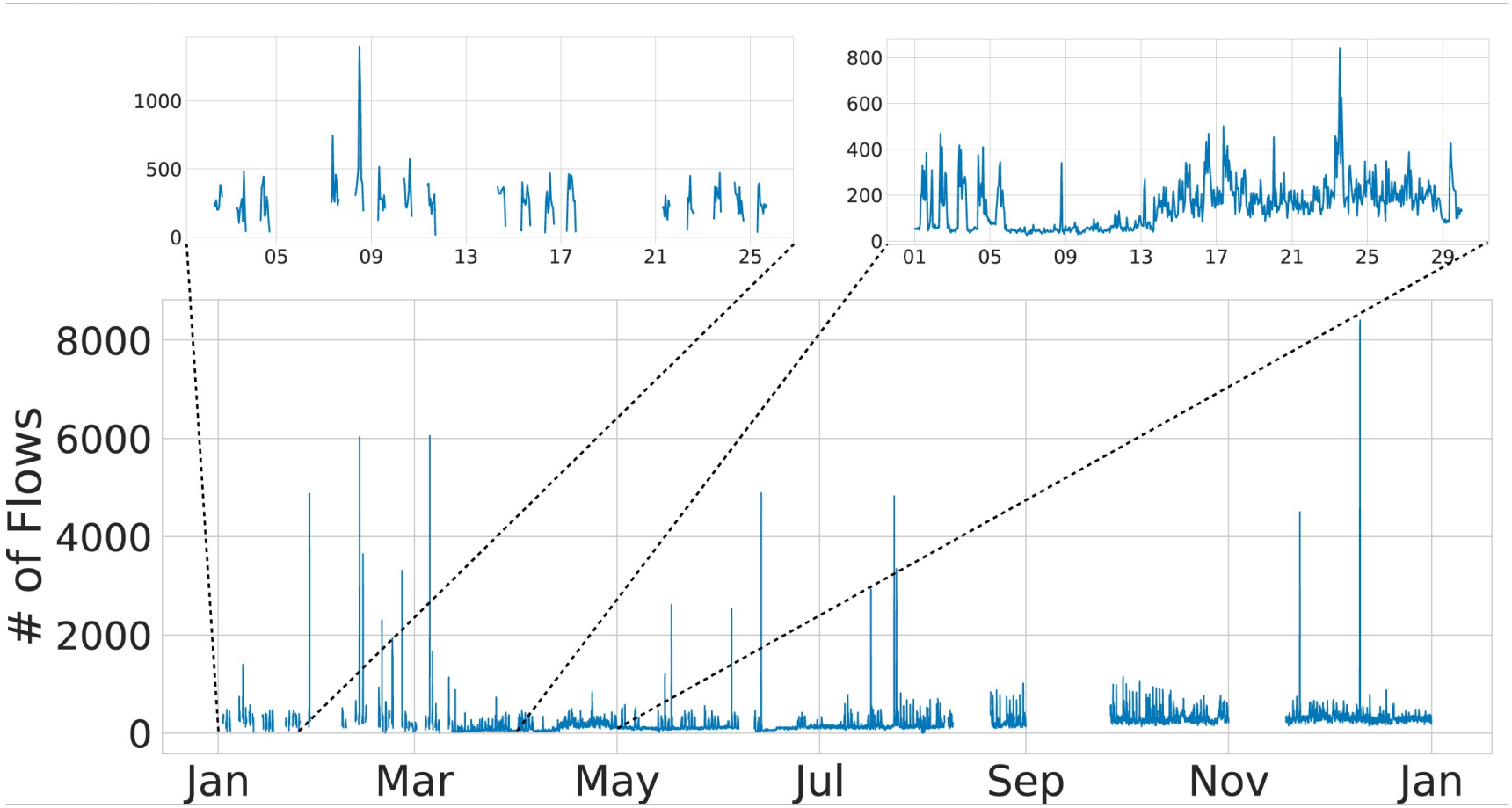
Detection of the increasing usage



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Profile Usecase III

Detection of the change in behavior



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Profile Usecase IV

Detection of the anomalous activity

- Example of the scanning detection
  - High number of flows
  - High number of distinct peers
  - Unchanged number of distinct ports

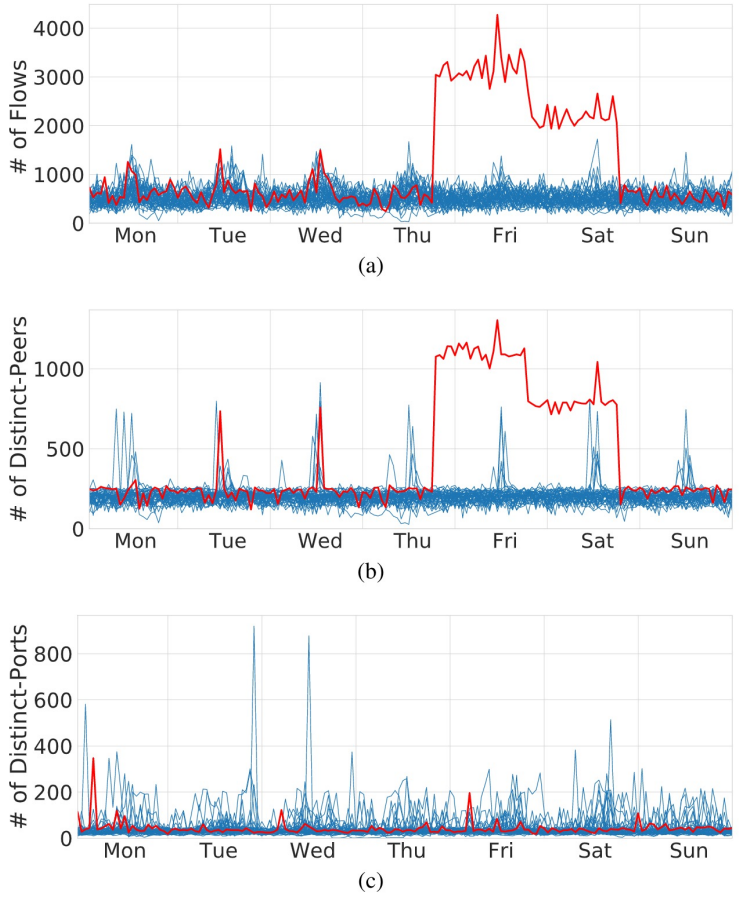


Fig. 14. Use case 3: Suspicious activity in week profile *(host 133.250.178.62)*, (a) number of flows, (b) number of distinct peers, (c) number of distinct ports.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

On-going: Automated Response

- Simple playbook for Phishing attacks
- The complexity is primarily within the performed actions
- Tip of the iceberg
  - Determine if quarantined email is Phishing
  - Get distributed OSINT for *IP*, *domain*, *file*
  - Search all traffic and logs for observables from 6 months ago
  - Block *IP* via FlowSpec, Block *domain* via DNS RPZ
- Orchestration is not overly hard, but also not trivial
  - We use *Apache Airflow* for our prototypes
  - Other engines are available

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Let’s get in touch

https://sappan-project.eu

https://csirt.muni.cz/

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833418