Real-time Detection of Malware Activities on Darknet by Estimating Anomalous Synchronization

Chansu Han

National Institute of Information and Communications Technology (NICT), Japan

FJ-cybersec2021: French Japanese Cybersecurity Intermediate Workshop 2021

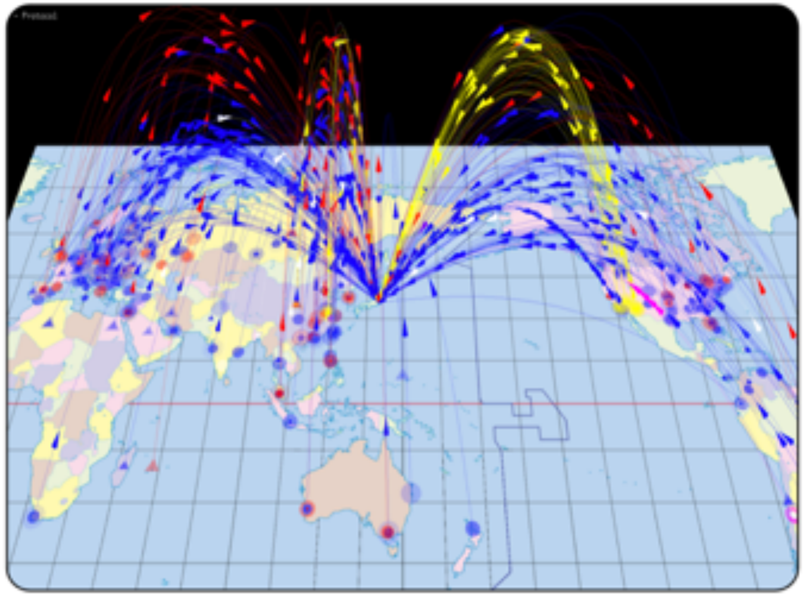
WG3, Feb 25-26, 2021

National Institute of Information and Communications Technology

Network Incident analysis Center for Tactical Emergency Response

Background - Darknet

- Darknet: unused IP address spaces on the Internet.
- Most of traffic that reach the darknet are malicious.
  - Many indiscriminate scan attacks from malware
  - But also harmless / benign scans (e.g., misconfig, shodan, ...)
- Only the initiation of a communication is observed.
- However, the intention of the communication
  can be roughly grasped by observing destination ports of each packet.



Visualization of darknet traffic, NICTER
https://www.nicter.jp/

Research Goal and Approach

- Research Goal

  Accurately detect potential malware activities in real-time from the myriad of indiscriminate scan attacks that reach the darknet.

- Research Approach

  We focused on the synchronization of spatiotemporal features of darknet traffic.

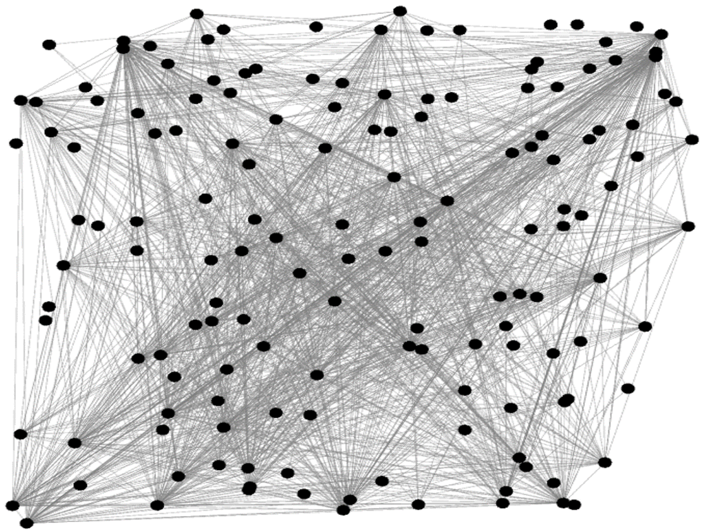
  - Devices infected with similar malware tend to scan in a similar spatiotemporal pattern to search for new infection targets.
  - We define hosts or ports scanned in a similar spatiotemporal pattern as synchronized.

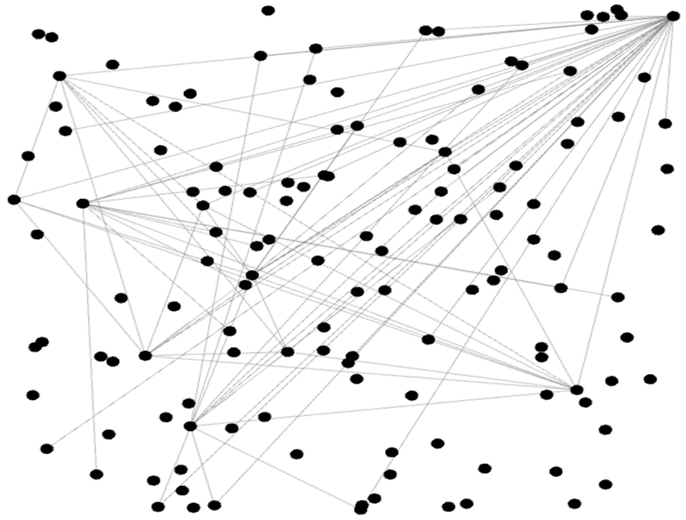
- Advantages
  - It is expected to eliminate unsynchronized noise traffic, such as misconfigured packets.
  - Malware activities can be detected if spatiotemporal features are highly synchronized, even if no clear spikes are seen.

Proposed Method 1: Sparse Structure Learning (Dark-GLASSO)

Outline of Dark-GLASSO

1. Applying the graphical lasso [1], it estimates conditional independence between spatial feature variables.
   - ✓ No relationship between two variables = independent when conditioned on all the other variables.
   - ✓ The relationships between spatial feature variables are sparsely estimated using the graphical lasso [1].
2. It quantifies and measures the degree of synchronized variables.
3. It compares the degree of synchronization in other time periods and detects outliers.





[1] J. Friedman, T. Hastie, and R. Tibshirani. "Sparse inverse covariance estimation with the graphical lasso," *Biostatistics*, Vol. 9, No. 3, pp. 432–441, 2008.

Proposed Method 2: Nonnegative Matrix Factorization (Dark-NMF)

Outline of Dark-NMF

1. Applying the Nonnegative Matrix Factorization (NMF) [2], it decomposes the spatiotemporal feature space into multiple potential time patterns and spatial patterns.
   - ✓ The NMF approximately decomposes the original matrix V into two smaller matrices W and H. ($V \cong WH$)
   - ✓ Confirm the same number of synchronized spatial feature groups as the number of bases to be decomposed.
2. It abnormally detects spatial features with high synchronization on the spatial patterns.

Algorithm 1 Multiplicative Update Algorithm on Dark-NMF

Require: Data matrix $V \in \mathbb{N}_0^{M \times N}$, rank parameter $r < \min(N, M)$, threshold stopping criterion ϵ, δ

Ensure: $W \in \mathbb{R}^{M \times r}$ and $H \in \mathbb{R}^{r \times N}$ $(V \approx WH)$

$\ell \leftarrow 0$

initialize $W^{(\ell)}$, $H^{(\ell)}$ by singular value decomposition

while $||V - WH||^2 < \epsilon$ or $\ell \geq \delta$ **do**

$\quad H^{(\ell+1)} \leftarrow H^{(\ell)} \frac{[(W^{(\ell)})^{\mathrm{T}} V]}{[(W^{(\ell)})^{\mathrm{T}} W^{(\ell)} H^{(\ell)}]}$

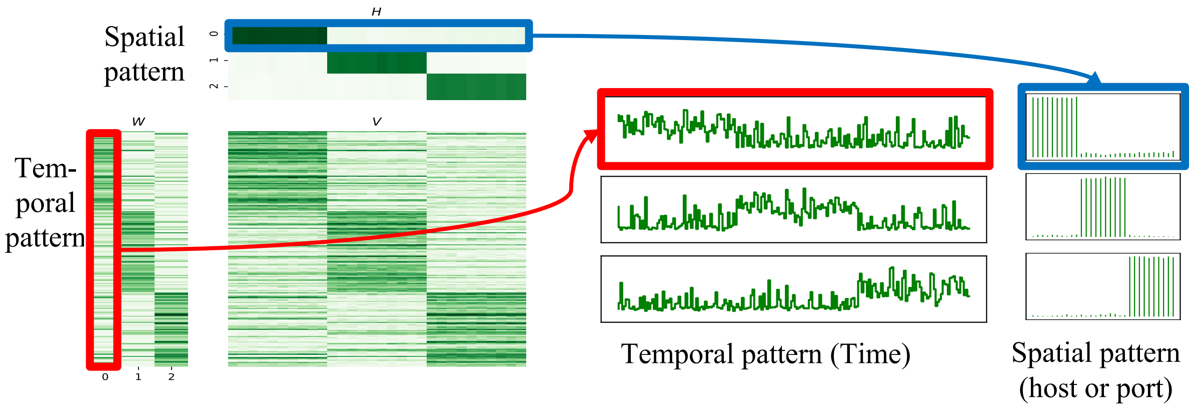
$\quad W^{(\ell+1)} \leftarrow W^{(\ell)} \frac{[(V H^{(\ell+1)})^{\mathrm{T}}]}{[W^{(\ell)} H^{(\ell+1)} (H^{(\ell+1)})^{\mathrm{T}}]}$

$\quad \ell \leftarrow \ell + 1$

end while

$W \leftarrow W^{(\ell)}$

$H \leftarrow H^{(\ell)}$



basis = 3

[2] Lee, Daniel D., and H. Sebastian Seung. "Algorithms for non-negative matrix factorization." *Advances in neural information processing systems (NIPS)*. 2000.

Input / Output of Proposed Methods

- Input Information
  - Value of Matrix V : the number of packets (non-negative integer value)
  - M : temporal feature (sampling the entire period of observation data into M pieces)
  - N : spatial feature (source IP addresses or destination port)

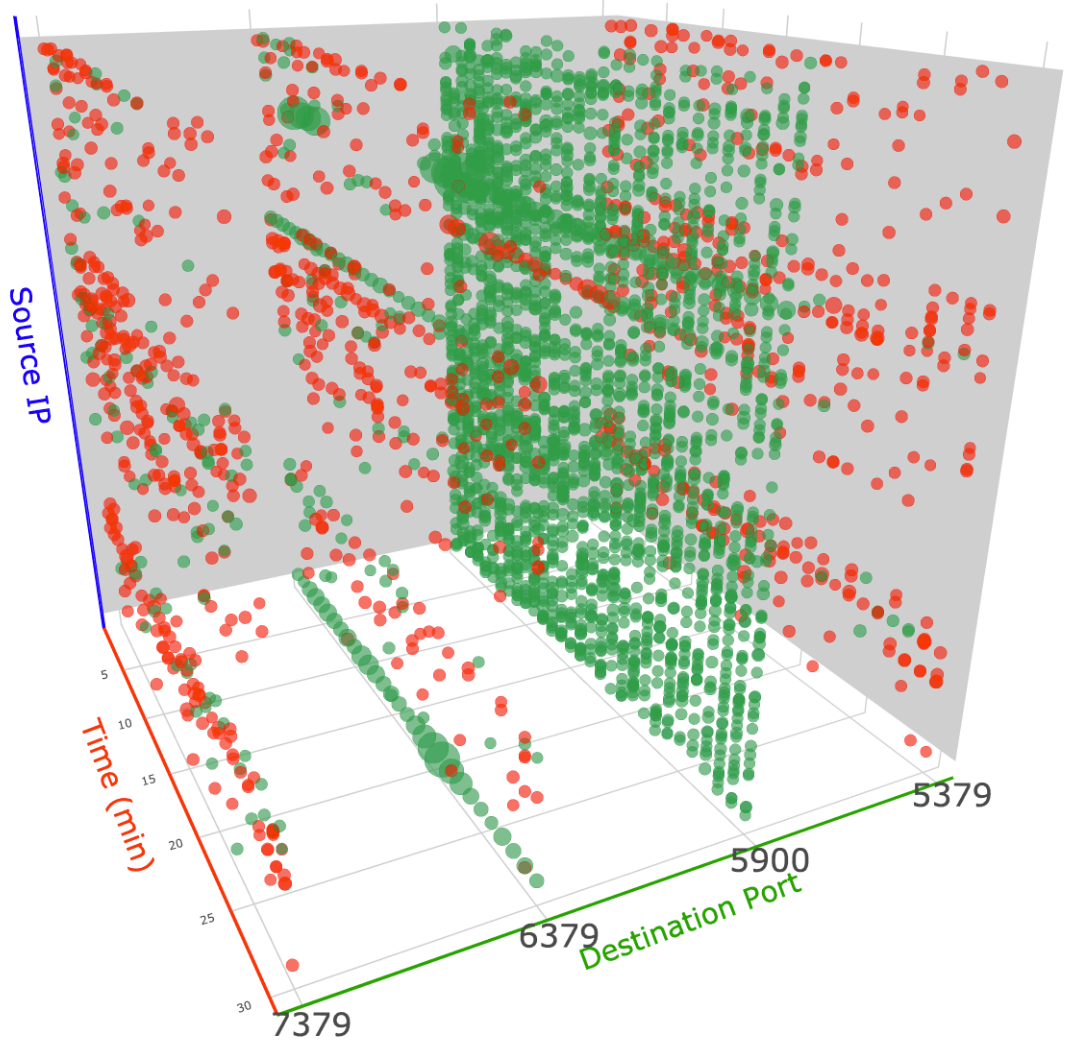
$$V \in \mathbb{N}_0^{M \times N}, \ \mathbb{N}_0 = \{0, \ 1, \ 2, \ \cdots\}$$

- Output Information

  Issue alerts include
  - timestamp
  - anomaly synchronized destination ports
  - anomaly synchronized IP addresses

Confirmation of Synchronization on Darknet

- Packets from the same host to different destination ports are observed at the same time are plotted in red.
- It is clarified that the three ports of 5379, 6379, and 7379 / TCP are strongly synchronized.
- In fact, attacks targeting Redis vulnerabilities were observed on those three ports in Oct 2018 [3].
- we confirmed many events that confirm actual states of such synchronization from alerts.



[3] Trend Micro, "**Exposed Redis Instances Abused for Remote Code Execution, Cryptocurrency Mining,**" Web blog, April, 2020.

Ground Truth of Malware Activities Observed in October 2018

Threat Type	Threat Group	TCP Port (include duplication)	Characteristics (observed from our darknets)
IoT Malware	Mirai I	82,83,84,85,88,8000, 8001,8081,8088,8888	About 1K hosts with the Mirai feature constantly probed our darknets. A spike of 6K hosts was observed on October 22.
	Mirai II	88,443,8081,8443	A spike of 7K hosts was observed on October 20 with the Mirai feature. Most packets originate from China, and the window size is fixed at 14100.
	Mirai Ⅲ	444,7547,8010	We observed spikes at different periods on each port with the Mirai feature (< 1K hosts). 7547/TCP: Most packets originate from Egypt. 444/TCP: Most packets originate from Greece.
	Hajime, *HNS* (Hide and Seek)	5358,9000 (Hajime), 2480,5984 (*HNS*)	Hajime: Over 1K hosts with the Hajime feature constantly probed our darknets. *HNS*: Over 2K hosts constantly probed our darknets [10].
Router Vulnerability	Manufacturer A	21,25,110,443,8291, 23023,65000	We observed spikes multiple times for each port from hosts that seemed to be products of router manufacturers A (about 6K hosts). The window size is fixed at 1024.
	Manufacturer B, C, D	37215 (B), 8181 (C), 8001,8081 (D)	We observed spikes for each port from hosts that seemed to be products of router manufacturers B, C, and D. They have the feature of Mirai.
	Manufacturer E	5431	We observed regular infection activities targeting the vulnerability of UPnP (Universal Plug and Play) of router manufacturer E in about 100K hosts [11].
Application Vulnerability	5 Vulnerabilities	1701 (L2TP VPN), 49152 (IPMI/BMC), 5900 (VNC), 2004 (WordPress), 5379,6379,7379(Redis)	1701: A spike of 3K hosts was observed on October 9 (from China). 49152: A spike of 6K hosts was observed on October 14 (from Egypt, Mirai feature). 5900: A spike of 4K hosts was observed on October 29 (window size = 8192). 2004: A spike of 300 hosts was observed on October 15 (window size = 14600, 29200). 5379,6379,7379: Spikes of 1K hosts were observed on October 31 for each port.

- Malware activities with similar characteristics are grouped based on TCP ports. (total of 35 TCP ports)

National Institute of Information and Communications Technology

Network Incident analysis Center for Tactical Emergency Response

Evaluation of Detection Performance of Malware Activities

- We evaluate how well methods can detect 35 TCP ports in the ground truth.
- ChangeFinder detects rapid change points with low calculation cost.
- Experiments were conducted with various parameter sets in Dark-NMF.
- This experiment is evaluated to reduce false negatives.

	Change Finder	**Dark-GLASSO**	**Dark-NMF**	
			SET1	SET2
True Positives	24	34	31	35
False Negatives	11	1	4	0
False Positives	0	0	9	1074
Recall (%) =TP/(TP+FN)	**68.6%**	**97.1%**	**88.6%**	**100%**

Malware Activity Detection Results of ChangeFinder, Dark-GLASSO, and Dark-NMF

Pros and Cons (Dark-GLASSO vs. Dark-NMF)

Dark-GLASSO	Dark-NMF
No false positives The overall accuracy is good.	Many false positives
It requires cubic time complexity. It is necessary to sample spatial features randomly.	It functions in linear time. Processing can be completed in real-time without sampling.
Accuracy decreases as the data size increases.	Even if the data size is large, the effect on accuracy is small.
Past data is required to recognize and detect abnormal features. (Parameter tuning cost is high.)	No past data is required to recognize and detect abnormal features. (Parameter tuning cost is low.)
Destination port feature space is too large to calculate	It can process both host and port feature spaces.

Pros = red
Cons = blue

Conclusion and Future Work

- Focusing on the synchronization of spatiotemporal features of darknet traffic, we propose Dark-GLASSO and Dark-NMF methods for detecting malware activities in real-time.
- As a result of quantitative evaluation, Dark-NMF answered all correctly although there were many false positives, and Dark-GLASSO recorded a high number of true positives without false positives.
- Dark-NMF has some advantages of system over Dark-GLASSO, such as calculation cost.
- We are currently testing real-time operation internally and plan to release the service in the future.
- Future work
  - Analyze detected alerts in detail and automatically annotate them.
  - Evaluate whether the time of detected alerts is appropriate or not.

Appendix

Background – Impact of IoT Malware

- A large number of attacks targeting IoT devices have been observed on the darknet (Fig. 1).
- A pandemic of IoT malware caused large-scale DDoS attacks.
- Cyberattacks by IoT malware are diversifying.

  The ratio of Telnet (23/TCP) is decreasing, and attacks on other service ports are increasing and diversifying.
- IoT malware is becoming more sophisticated.

  Several IoT malware with "persistent infectivity" that are not deleted even when the device is turned off has been discovered.

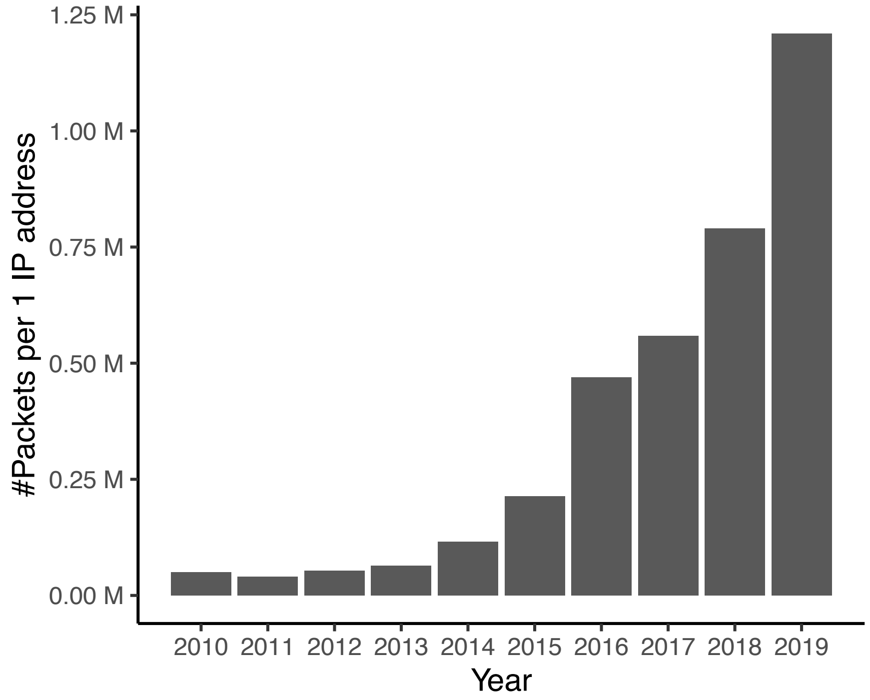
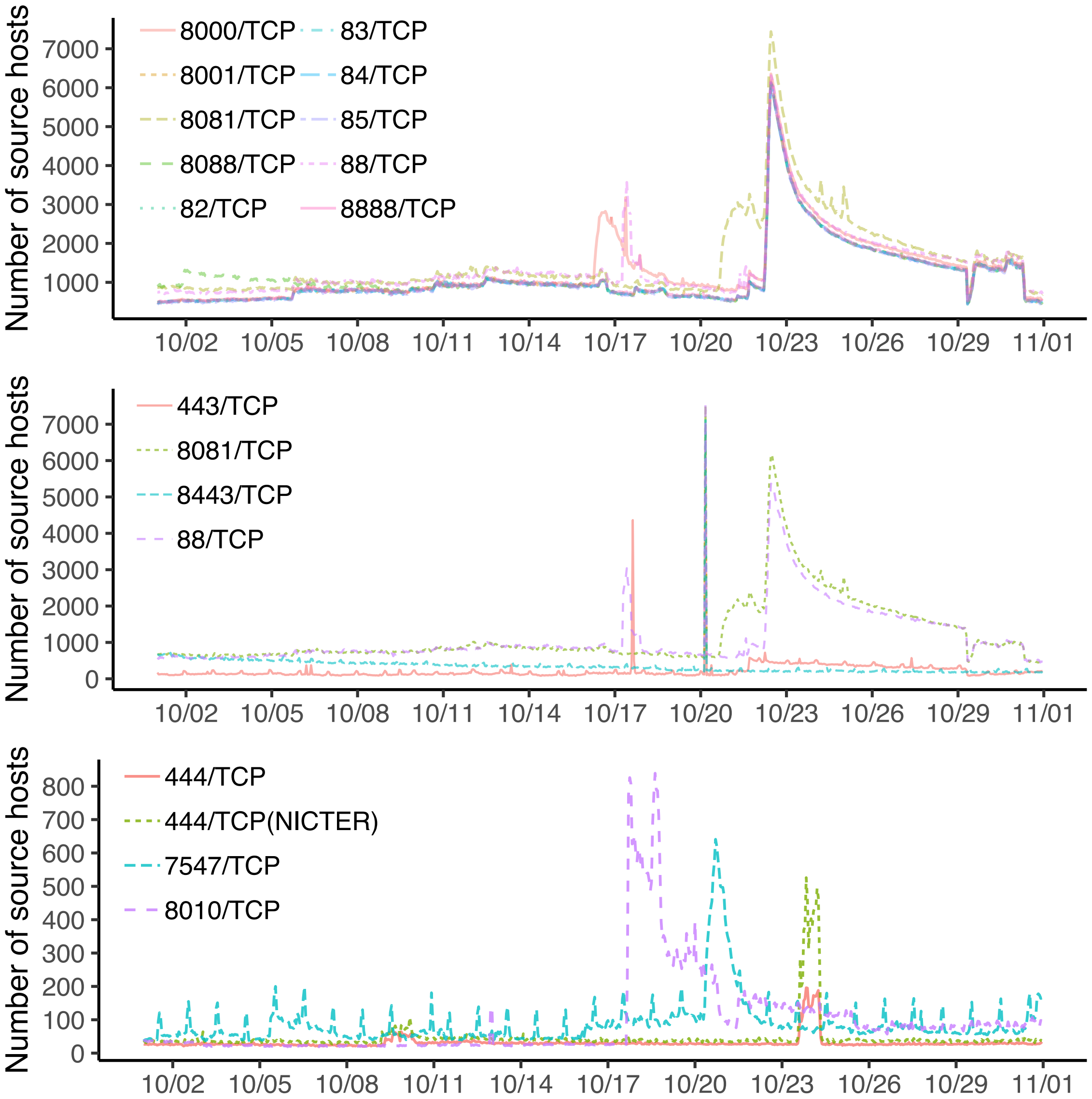


Fig 1. Number of packets observed per IP address on the NICTER darknet

Number of Unique Source Hosts per Hour in Oct 2018

Mirai



Router, Application Vulnerabilities