ASSESSING INTERNET-WIDE CYBER SITUATIONAL AWARENESS OF CRITICAL SECTORS

Thursday 30th August, 2018

Martin Husák
Nataliia Neshenko
Morteza Safaei Pour
Elias Bou-Harb
Pavel Čeleda

FAU
CYBER THREAT INTELLIGENCE LAB
College of Engineering & Computer Science
Florida Atlantic University

CSIRT-MU

Motivation

Sector-specific malware

- Rise of IoT and CPS paradigms in critical sectors,
- Stuxnet, Havex, Industroyer, . . .

Wide-area cyber situational awareness

- Global remediation objectives.
- It is too laborious to obtain network traffic traces from various sectors, even on a smaller scale.
- Unwillingness of certain sectors to share cyber security information (banking sector – fear of brand damage).

Research Questions

Question I.

Given the lack of empirical data that can be analyzed from within various sectors, including critical infrastructure, in addition to the complementary logistics and privacy issues, how can one assess the Internet-scale cyber security posture of such sectors?

Question II.

What insights and inferences can one generate by analyzing and characterizing sector-related empirical data, which could be used for effective cyber threat intelligence

Proposed Approach

Collecting Darknet Data

Darknet

- CAIDA /8 darknet.
- Macroscopic – 1/256 of the total IP address range.

Data Processing

- Darknet flow – series of consecutive packets from the same source IP address.
- Other characteristics – IP protocol, port number, TCP flags.
- Threshold-based methods of scan and DDoS backscatter detection (64 packets per event).

Sector Attribution

Manual attribution

- DNS and WHOIS querying,
- too laborious and time-consuming.

Automated attribution

- Collaborative effort to access and collect private information on IP blocks.
- Database of sector information per IP blocks, similar to geolocation databases.
- Limited public access as of today.

Identifying Critical Sectors

- Manual identification of critical sectors using DHS and EU lists.
- EU Council Directive 2008/114/EC defines European Critical Infrastructure covering mostly Energy and Transport.
- Department of Homeland Security defines 16 critical sectors:

Chemical	Financial Services
Commercial Facilities	Food and Agriculture
Communications	Government Facilities
Critical Manufacturing	Healthcare and Public Health
Dams	Information Technology
Defense Industrial Base	Nuclear Reactors, Materials, and Waste
Emergency Services	Transportation Systems
Energy	Water and Wastewater Systems

Data Analysis

Scan-to-DDoS Ratio

- Ratio of network scanning to DDoS attacks, computed from the share of a given sector's scan and DDoS attacks.
- Network scanning indicates infected hosts.
- DDoS attack indicate highly interesting targets.

Interpretation

- Below-average ratio – many infected hosts of less significance.
- Above-average ratio – better secured (critical?) hosts, more likely to be DDoS targets.

Empirical Evaluation

Collected Data

Measurement

- 16.8 TB of darknet data,
- 1 week of measurement.

Inferred events

- 8M network scanning events per day,
- 1.8M distinct scanning IPs per day,
- 30k DDoS attacks per day,
- 7k distinct DDoS victim IPs per day.

Critical Sector Attribution

Sector attribution

- Successful for **86.73%** of events – **92.08%** distinct IP addresses,
- Discrepancy between unknown sectors:
  scans – **13.14%**, DDoS backscatter – **31.70%**.
- Large share of Telecommunications and ISP sectors.

Critical sectors

- Manual scrutinization of critical sectors.
- No available machine-readable lists.
- 49 different sectors, 6 of them critical.
- Share of critical sectors is **less than 1%**
  (both scans and DDoS backscatter).

Scan to DDoS Ratio

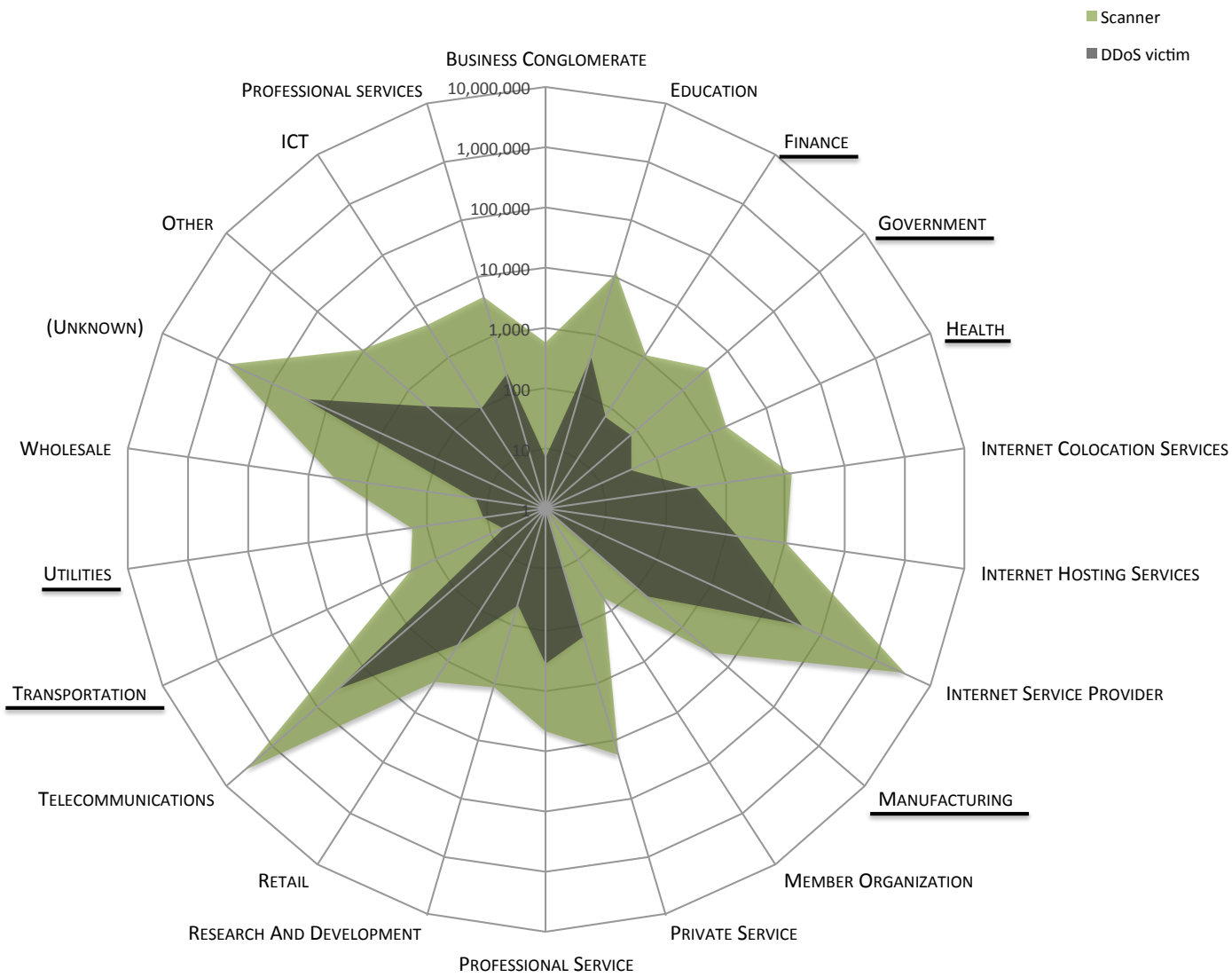
Illustrative Examples

- Telecommunications and ISPs – above average.
- Internet hosting service – bellow average.

Critical Sectors

- Should be similar to Internet hosting services.
- Financial sector, Manufacturing, and Utilities conform to this.
- Government, Health, Transportation – around-average ratio!
- No critical sector with significantly higher ratio.

Scanners and DDoS victims per sector



Scan to DDoS share ratio of top-10 sectors

Sector	Scans (%)	DDoS (%)	Ratio
Telecommunications	47.668	33.049	1.442
Internet Service Provider	43.404	40.583	1.069
(unknown)	7.717	22.505	0.343
Private Service	0.224	0.134	1.671
Internet Colocation Services	0.157	0.292	0.538
Education	0.154	0.388	0.397
Internet Hosting Services	0.135	1.351	0.100
Other	0.137	0.341	0.402
Professional Service	0.059	0.314	0.187
ICT	0.053	0.085	0.623
Average ratio (all sectors)			**0.681**

Scan to DDoS share ratio of critical sectors

Sector	Scans (%)	DDoS (%)	Ratio
Manufacturing	0.053	0.139	0.383
Government	0.044	0.064	0.693
Health	0.024	0.032	0.736
Finance	0.014	0.056	0.247
Transportation	0.004	0.005	0.684
Utilities	0.002	0.010	0.219
All critical sectors combined	0.140	0.306	0.460
Average ratio (all sectors)			**0.681**

Conclusion and Future Work

Conclusion

- Week-long measurements of darknet traffic (global scope).
- Attribution of IP addresses of scanners and DDoS victims with their corresponding sectors.
- Identification of critical sectors.
- Scan-to-DDoS ratio characterizing sectors.

Future Work

- Characteristics of (critical) sectors – device types and network services unique to a given sector,
- Long-term monitoring and trend analysis.

THANK YOU FOR YOUR ATTENTION!

csirt.muni.cz

@csirtmu

Martin Husák

husakm@ics.muni.cz

FAU

CYBER THREAT INTELLIGENCE LAB

College of Engineering & Computer Science
Florida Atlantic University

CSIRT-MU