

Cyber Event Database Report

By Ethan Prendergast

SQL Scripts:

- create.sql
- insert.sql
- drop.sql
- queries.sql

Documentation:

- Database Schema
- Database Population
- Non-Trivial Query 1
- Reflection Query 1
- Comprehensive Test Data 1
- Non-Trivial Query 2
- Reflection Query 2
- Comprehensive Test Data 2

Database Schema

The describe command shows a description of the table's schema

- 1 • `describe naics;`
- 2 • `describe isocc;`
- 3 • `describe cyber_events;`
- 4 • `describe event_subtypes;`

Naics

Field	Type	Null	Key	Default	Extra
naics_code	int	NO	PRI	NULL	
naics_description	varchar(255)	YES		NULL	

Isocc

Field	Type	Null	Key	Default	Extra
c_code	char(3)	NO	PRI	NULL	
c_name	varchar(255)	NO		NULL	

Cyber_events

Field	Type	Null	Key	Default	Extra
e_id	char(16)	NO	PRI	NULL	
e_date	char(10)	NO		NULL	
e_year	int	NO		NULL	
e_month	int	NO		NULL	
actor	varchar(100)	NO		NULL	
actor_type	varchar(50)	NO		NULL	
organization	varchar(100)	NO		NULL	
industry_code	int	NO	MUL	NULL	
motive	varchar(50)	NO		NULL	
e_type	char(20)	NO		NULL	
e_description	varchar(500)	NO		NULL	
source_url	varchar(200)	NO		NULL	
target_country	char(3)	NO	MUL	NULL	
actor_country	char(3)	NO	MUL	NULL	

Event_sybtypes


Field	Type	Null	Key	Default	Extra
e_id	char(16)	NO	PRI	NULL	
e_subtype	varchar(50)	NO	PRI	NULL	

Database Population

The following queries show the number of tuples in each table

```
# table populations
select count(*) AS industries from naics;
select count(*) AS countries from isocc;
select count(*) AS events from cyber_events;
select count(*) AS events_and_subtypes from event_subtypes;
```

Result Grid			Filter Rows: <input type="text"/>	Export: 	Wrap Cell Content: 
	industries				
▶	11				

Result Grid			Filter Rows: <input type="text"/>	Export: 	Wrap Cell Content: 
	countries				
▶	13				

Result Grid			Filter Rows: <input type="text"/>	Export: 	Wrap Cell Content: 
	events				
▶	27				

Result Grid			Filter Rows: <input type="text"/>	Export: 	Wrap Cell Content: 
	events_and_subtypes				
▶	30				

(There are more tuples in event_subtypes as some attacks were mixed, and had several subtypes for one event)

Non-Trivial Query 1

For each cyber event where the actor country is USA, list the event information.

Order the results by target country name and for the same target country, order the results by the event date
(target_country_name, e_date, e_id, e_type, industry_description, motive)

Query

```
select c_name target_country_name, e_date, e_id, e_type, naics_description industry_description, motive
from naics N join (cyber_events CE join isocc I on CE.target_country = I.c_code) on N.naics_code =
CE.industry_code

where CE.actor_country = 'USA'

order by CE.target_country, CE.e_date DESC;
```

Answer

Result Grid						
		Filter Rows:	Export:		Wrap Cell Content:	
	target_country_name	e_date	e_id	e_type	industry_description	motive
▶	Iran (Islamic Republic of)	2024-02-15	47f00a8ccc43d5da	Disruptive	Transportation and Warehousing	Sabotage
	Russian Federation	2024-02-14	ea1304bf4b5116d6	Disruptive	Public Administration	Undetermined
	United States of America	2024-04-03	2d89a9ffc0ae60c9	Exploitive	Undetermined	Espionage

Reflection Query 1

The following query shows the total list of cyber_events with actor countries. Events with USA as the actor country are highlighted in red

Query

```
select c_name target_country_name, e_date, e_id, e_type, naics_description industry_description, motive, actor_country
from naics N join (cyber_events CE join isocc I on CE.target_country = I.c_code) on N.naics_code = CE.industry_code;
```

Answer

Result Grid							
Filter Rows:		Export:		Wrap Cell Content:			
	target_country_name	e_date	e_id	e_type	industry_description	motive	actor_country
▶	Ukraine	2024-01-25	006f7f1a20156254	Disruptive	Utilities	Sabotage	UND
	United States of America	2024-01-16	60c10acd4e7407c6	Disruptive	Utilities	Undetermined	RUS
	Lebanon	2024-09-26	a05b194a6a6d9701	Disruptive	Utilities	Sabotage	ISR
	United States of America	2024-03-06	c25a87e8cf43fa59	Exploitive	Retail Trade	Financial	UND
	Estonia	2024-04-25	27ac800a4c7a20ea	Disruptive	Transportation and Warehousing	Sabotage	RUS
	Iran (Islamic Republic of)	2024-02-15	47f00a8ccc43d5da	Disruptive	Transportation and Warehousing	Sabotage	USA
	United States of America	2024-01-23	58340973ee0c5732	Mixed	Transportation and Warehousing	Financial	UND
	Undetermined	2024-06-28	65e07ba91f3d29c8	Exploitive	Transportation and Warehousing	Financial	UND
	Russian Federation	2024-01-09	430028dee10aff28	Disruptive	Information	Protest	UKR
	United States of America	2024-03-01	74ab0e2986e5a54b	Exploitive	Information	Financial	UND
	Ukraine	2024-01-02	897793b71365a2ff	Exploitive	Information	Sabotage	RUS
	United States of America	2024-05-21	d8c669598a1c1d6e	Exploitive	Information	Financial	UND
	Ukraine	2024-03-19	ef172bf0779be9d7	Mixed	Information	Sabotage	RUS
	Iran (Islamic Republic of)	2024-08-14	ft8770g40e9gqxu4	Exploitive	Finance and Insurance	Financial	UND
	Undetermined	2024-09-02	1a223c9e04046912	Exploitive	Professional, Scientific, and Tec...	Undetermined	UND
	United States of America	2024-02-14	88963111a5a550d1	Disruptive	Professional, Scientific, and Tec...	Protest	RUS
	Australia	2024-01-22	b9a7924fd4fdeb37	Exploitive	Professional, Scientific, and Tec...	Financial	UND
	Russian Federation	2024-04-10	9016f06fda573322	Exploitive	Administrative and Support and ...	Protest	UKR
	United States of America	2024-05-08	01e9862f655cfd85	Mixed	Health Care and Social Assistance	Financial	RUS
	United States of America	2024-06-28	3d71ca29f703ffbc	Mixed	Health Care and Social Assistance	Financial	UND
	Israel	2024-01-23	668228a28ac0743e	Disruptive	Arts, Entertainment, and Recre...	Protest	TUR
	United Kingdom of Grea...	2024-03-14	60b86709daca0f54	Disruptive	Public Administration	Sabotage	UND
	Canada	2024-03-05	779bbcc0aa08950b	Disruptive	Public Administration	Financial	UND
	United States of America	2024-01-18	89e7cc0b666aff40	Mixed	Public Administration	Financial	UND
	Colombia	2024-01-26	b0d16e97f2a79f1e	Disruptive	Public Administration	Financial	UND
	Russian Federation	2024-02-14	ea1304bf4b5116d6	Disruptive	Public Administration	Undetermined	USA
	United States of America	2024-04-03	2d89a9ffc0ae60c9	Exploitive	Undetermined	Espionage	USA

Comprehensive Data 1

The following query shows each country that was an actor in a cyber event, and how many times they were an actor in a cyber event. The second answer shown is the reflection query highlighted to also showcase the number of times Ukraine was an actor

Query **select** c_code country_code, c_name country_name, count(*) AS actorInstances
from isocc l join cyber_events CE on l.c_code = CE.actor_country
group by c_code;

Answer

country_code	country_name	actorInstances
ISR	Israel	1
RUS	Russian Federation	6
TUR	Turkey	1
UKR	Ukraine	2
UND	Undetermined	14
USA	United States of America	3

target_country_name	e_date	e_id	e_type	industry_description	motive	actor_country
Ukraine	2024-01-25	006f7f1a20156254	Disruptive	Utilities	Sabotage	UND
United States of America	2024-01-16	60c10acd4e7407c6	Disruptive	Utilities	Undetermined	RUS
Lebanon	2024-09-26	a05b194a6a6d9701	Disruptive	Utilities	Sabotage	ISR
United States of America	2024-03-06	c25a87e8cf43fa59	Exploitive	Retail Trade	Financial	UND
Estonia	2024-04-25	27ac800a4c7a20ea	Disruptive	Transportation and Warehousing	Sabotage	RUS
Iran (Islamic Republic of)	2024-02-15	47f00a8ccc43d5da	Disruptive	Transportation and Warehousing	Sabotage	USA
United States of America	2024-01-23	58340973ee0c5732	Mixed	Transportation and Warehousing	Financial	UND
Undetermined	2024-06-28	65e07ba91f3d29c8	Exploitive	Transportation and Warehousing	Financial	UND
Russian Federation	2024-01-09	430028dee10aff28	Disruptive	Information	Protest	UKR
United States of America	2024-03-01	74ab0e2986e5a54b	Exploitive	Information	Financial	UND
Ukraine	2024-01-02	897793b71365a2ff	Exploitive	Information	Sabotage	RUS
United States of America	2024-05-21	d8c669598a1c1d6e	Exploitive	Information	Financial	UND
Ukraine	2024-03-19	ef172bf0779be9d7	Mixed	Information	Sabotage	RUS
Iran (Islamic Republic of)	2024-08-14	ft8770g40e9gqxu4	Exploitive	Finance and Insurance	Financial	UND
Undetermined	2024-09-02	1a223c9e04046912	Exploitive	Professional, Scientific, and Tec...	Undetermined	UND
United States of America	2024-02-14	88963111a5a550d1	Disruptive	Professional, Scientific, and Tec...	Protest	RUS
Australia	2024-01-22	b9a7924fd4fdeb37	Exploitive	Professional, Scientific, and Tec...	Financial	UND
Russian Federation	2024-04-10	9016f06fda573322	Exploitive	Administrative and Support and ...	Protest	UKR
United States of America	2024-05-08	01e9862f655cf885	Mixed	Health Care and Social Assistance	Financial	RUS
United States of America	2024-06-28	3d71ca29f703ffbc	Mixed	Health Care and Social Assistance	Financial	UND
Israel	2024-01-23	668228a28ac0743e	Disruptive	Arts, Entertainment, and Recre...	Protest	TUR
United Kingdom of Grea...	2024-03-14	60b86709daca0f54	Disruptive	Public Administration	Sabotage	UND
Canada	2024-03-05	779bbcc0aa08950b	Disruptive	Public Administration	Financial	UND
United States of America	2024-01-18	89e7cc0b666aff40	Mixed	Public Administration	Financial	UND
Colombia	2024-01-26	b0d16e97f2a79f1e	Disruptive	Public Administration	Financial	UND
Russian Federation	2024-02-14	ea1304bf4b5116d6	Disruptive	Public Administration	Undetermined	USA
United States of America	2024-04-03	2d89a9ffc0ae60c9	Exploitive	Undetermined	Espionage	USA

Test data shows that the number of actor countries is varied with 6 unique actor countries, and the count provided for the NTQ is accurate.

Non-Trivial Query 2

For each event subtype appearing in the event_subtypes table, determine the number of events with that subtype. Order the results so that the event subtype with the most events is listed first and for those having the same number of events, order the results alphabetically by event subtype

(event_subtype, numberOfEvents)

Query

```
select e_subtype event_subtype, count(*) AS numberOfEvents
from event_subtypes
group by e_subtype
order by numberOfEvents DESC , e_subtype;
```

Answer

Result Grid			Filter Rows:	Export:	Wrap Cell Content:
	event_subtype	numberOfEvents			
▶	Exploitation of Application Server	6			
	Data Attack	5			
	Physical Attack	4			
	Message Manipulation	3			
	Undetermined	3			
	Exploitation of End Host	2			
	Exploitation of Network Infrastructure	2			
	External Denial of Service	2			
	Exploitation of Data in Transit	1			
	Exploitation of Sensors	1			
	Internal Denial of Service	1			

Reflection Query 2

Illustrates the events and their subtypes																																																																															
Query	select * from event_subtypes order by e_subtype;																																																																														
Answer	<div><div>Result Grid</div><div><div>Filter Rows:</div><div>Edit:</div><div>Export/Import:</div><div>Wrap Cell Content:</div></div><table><thead><tr><th>e_id</th><th>e_subtype</th><th></th></tr></thead><tbody><tr><td>01e9862f655cfd85</td><td>Data Attack</td><td rowspan="5">4</td></tr><tr><td>89e7cc0b666aff40</td><td>Data Attack</td></tr><tr><td>3d71ca29f703ffbc</td><td>Data Attack</td></tr><tr><td>430028dee10aff28</td><td>Data Attack</td></tr><tr><td>58340973ee0c5732</td><td>Data Attack</td></tr><tr><td>ft8770g40e9gqxu4</td><td>Exploitation of Application Server</td><td rowspan="6">6</td></tr><tr><td>d8c669598a1c1d6e</td><td>Exploitation of Application Server</td></tr><tr><td>89e7cc0b666aff40</td><td>Exploitation of Application Server</td></tr><tr><td>74ab0e2986e5a54b</td><td>Exploitation of Application Server</td></tr><tr><td>58340973ee0c5732</td><td>Exploitation of Application Server</td></tr><tr><td>01e9862f655cfd85</td><td>Exploitation of Application Server</td></tr><tr><td>65e07ba91f3d29c8</td><td>Exploitation of Data in Transit</td><td>1</td></tr><tr><td>c25a87e8cf43fa59</td><td>Exploitation of End Host</td><td rowspan="2">2</td></tr><tr><td>2d89a9ffc0ae60c9</td><td>Exploitation of End Host</td></tr><tr><td>b9a7924fd4fdeb37</td><td>Exploitation of Network Infrastr...</td><td rowspan="2">2</td></tr><tr><td>1a223c9e04046912</td><td>Exploitation of Network Infrastr...</td></tr><tr><td>9016f06fda573322</td><td>Exploitation of Sensors</td><td>1</td></tr><tr><td>006f7f1a20156254</td><td>External Denial of Service</td><td rowspan="2">2</td></tr><tr><td>88963111a5a550d1</td><td>External Denial of Service</td></tr><tr><td>779bbcc0aa08950b</td><td>Internal Denial of Service</td><td>1</td></tr><tr><td>b0d16e97f2a79f1e</td><td>Message Manipulation</td><td rowspan="3">3</td></tr><tr><td>668228a28ac0743e</td><td>Message Manipulation</td></tr><tr><td>ea1304bf4b5116d6</td><td>Message Manipulation</td></tr><tr><td>27ac800a4c7a20ea</td><td>Physical Attack</td><td rowspan="4">4</td></tr><tr><td>a05b194a6a6d9701</td><td>Physical Attack</td></tr><tr><td>60c10acd4e7407c6</td><td>Physical Attack</td></tr><tr><td>60b86709daca0f54</td><td>Physical Attack</td></tr><tr><td>897793b71365a2ff</td><td>Undetermined</td><td rowspan="3">3</td></tr><tr><td>ef172bf0779be9d7</td><td>Undetermined</td></tr><tr><td>47f00a8ccc43d5da</td><td>Undetermined</td></tr><tr><td>NULL</td><td>NULL</td><td></td></tr></tbody></table></div>		e_id	e_subtype		01e9862f655cfd85	Data Attack	4	89e7cc0b666aff40	Data Attack	3d71ca29f703ffbc	Data Attack	430028dee10aff28	Data Attack	58340973ee0c5732	Data Attack	ft8770g40e9gqxu4	Exploitation of Application Server	6	d8c669598a1c1d6e	Exploitation of Application Server	89e7cc0b666aff40	Exploitation of Application Server	74ab0e2986e5a54b	Exploitation of Application Server	58340973ee0c5732	Exploitation of Application Server	01e9862f655cfd85	Exploitation of Application Server	65e07ba91f3d29c8	Exploitation of Data in Transit	1	c25a87e8cf43fa59	Exploitation of End Host	2	2d89a9ffc0ae60c9	Exploitation of End Host	b9a7924fd4fdeb37	Exploitation of Network Infrastr...	2	1a223c9e04046912	Exploitation of Network Infrastr...	9016f06fda573322	Exploitation of Sensors	1	006f7f1a20156254	External Denial of Service	2	88963111a5a550d1	External Denial of Service	779bbcc0aa08950b	Internal Denial of Service	1	b0d16e97f2a79f1e	Message Manipulation	3	668228a28ac0743e	Message Manipulation	ea1304bf4b5116d6	Message Manipulation	27ac800a4c7a20ea	Physical Attack	4	a05b194a6a6d9701	Physical Attack	60c10acd4e7407c6	Physical Attack	60b86709daca0f54	Physical Attack	897793b71365a2ff	Undetermined	3	ef172bf0779be9d7	Undetermined	47f00a8ccc43d5da	Undetermined	NULL	NULL	
e_id	e_subtype																																																																														
01e9862f655cfd85	Data Attack	4																																																																													
89e7cc0b666aff40	Data Attack																																																																														
3d71ca29f703ffbc	Data Attack																																																																														
430028dee10aff28	Data Attack																																																																														
58340973ee0c5732	Data Attack																																																																														
ft8770g40e9gqxu4	Exploitation of Application Server	6																																																																													
d8c669598a1c1d6e	Exploitation of Application Server																																																																														
89e7cc0b666aff40	Exploitation of Application Server																																																																														
74ab0e2986e5a54b	Exploitation of Application Server																																																																														
58340973ee0c5732	Exploitation of Application Server																																																																														
01e9862f655cfd85	Exploitation of Application Server																																																																														
65e07ba91f3d29c8	Exploitation of Data in Transit	1																																																																													
c25a87e8cf43fa59	Exploitation of End Host	2																																																																													
2d89a9ffc0ae60c9	Exploitation of End Host																																																																														
b9a7924fd4fdeb37	Exploitation of Network Infrastr...	2																																																																													
1a223c9e04046912	Exploitation of Network Infrastr...																																																																														
9016f06fda573322	Exploitation of Sensors	1																																																																													
006f7f1a20156254	External Denial of Service	2																																																																													
88963111a5a550d1	External Denial of Service																																																																														
779bbcc0aa08950b	Internal Denial of Service	1																																																																													
b0d16e97f2a79f1e	Message Manipulation	3																																																																													
668228a28ac0743e	Message Manipulation																																																																														
ea1304bf4b5116d6	Message Manipulation																																																																														
27ac800a4c7a20ea	Physical Attack	4																																																																													
a05b194a6a6d9701	Physical Attack																																																																														
60c10acd4e7407c6	Physical Attack																																																																														
60b86709daca0f54	Physical Attack																																																																														
897793b71365a2ff	Undetermined	3																																																																													
ef172bf0779be9d7	Undetermined																																																																														
47f00a8ccc43d5da	Undetermined																																																																														
NULL	NULL																																																																														

Comprehensive Data 2

Illustrates each unique event subtype present in the table																									
Query	select distinct e_subtype from event_subtypes;																								
Answer	<div><div>Result Grid</div><div><div>Filter Rows:</div><div>Export:</div><div>Wrap Cell Content:</div></div><table><thead><tr><th></th><th>e_subtype</th></tr></thead><tbody><tr><td>▶</td><td>External Denial of Service</td></tr><tr><td></td><td>Data Attack</td></tr><tr><td></td><td>Exploitation of Application Server</td></tr><tr><td></td><td>Exploitation of Network Infrastructure</td></tr><tr><td></td><td>Physical Attack</td></tr><tr><td></td><td>Exploitation of End Host</td></tr><tr><td></td><td>Undetermined</td></tr><tr><td></td><td>Exploitation of Data in Transit</td></tr><tr><td></td><td>Message Manipulation</td></tr><tr><td></td><td>Internal Denial of Service</td></tr><tr><td></td><td>Exploitation of Sensors</td></tr></tbody></table></div>		e_subtype	▶	External Denial of Service		Data Attack		Exploitation of Application Server		Exploitation of Network Infrastructure		Physical Attack		Exploitation of End Host		Undetermined		Exploitation of Data in Transit		Message Manipulation		Internal Denial of Service		Exploitation of Sensors
	e_subtype																								
▶	External Denial of Service																								
	Data Attack																								
	Exploitation of Application Server																								
	Exploitation of Network Infrastructure																								
	Physical Attack																								
	Exploitation of End Host																								
	Undetermined																								
	Exploitation of Data in Transit																								
	Message Manipulation																								
	Internal Denial of Service																								
	Exploitation of Sensors																								
Test data shows that all 11 subtypes are present in the table, meaning that every subtype is represented in the data at least once.																									