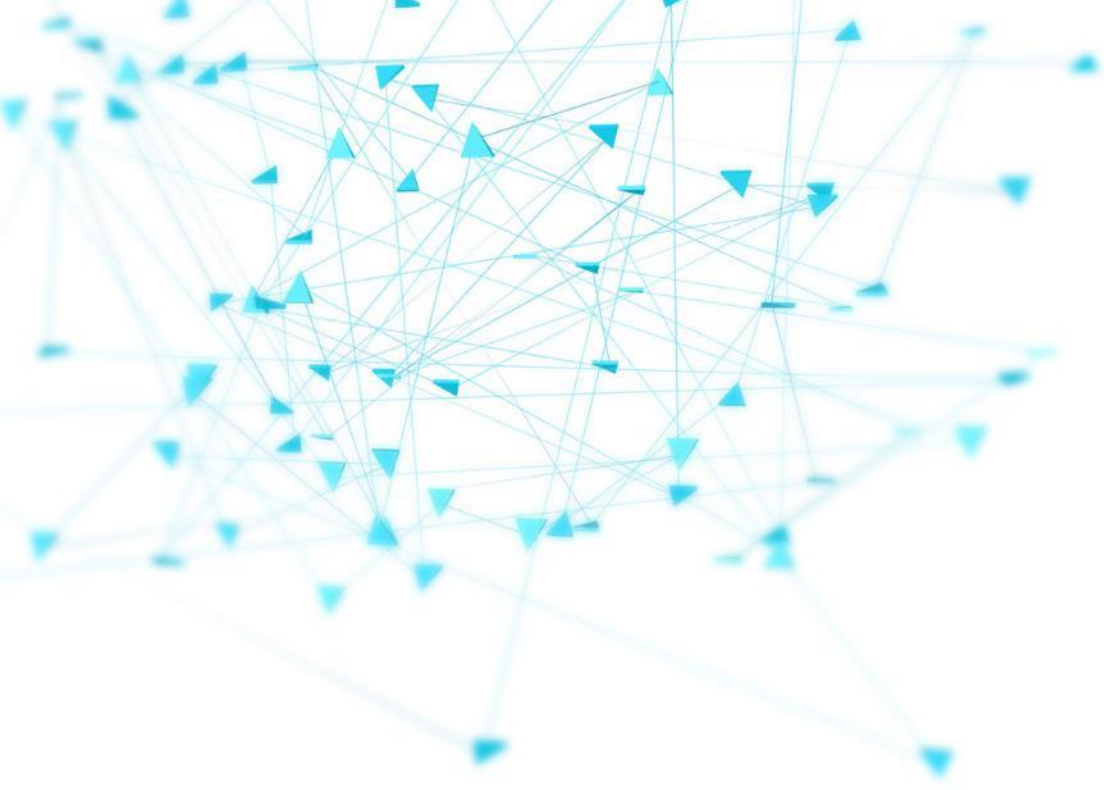


TOVEK

Využití AI pro analýzu šifrovaného síťového provozu

find ▸
understand ▸
use ▸

Proč analyzovat šifrovanou komunikaci?

TOVEK

- Analýza komunikace mezi zájmovými subjekty
  - Jaké aplikace pro komunikaci používají?
  - V jakém čase a z jakých míst komunikují
  - Jaké používají IP adresy / zařízení
- Profilování určitého subjektu / IP adresy
  - Jaké aplikace používá?
  - V jakém čase a z jakých míst komunikuje
- Forenzní analýza zachyceného provozu
  - Identifikace zájmové komunikace na základě aplikace, času…
  - … pro výběr a podrobnou analýzu dat z dalších zdrojů

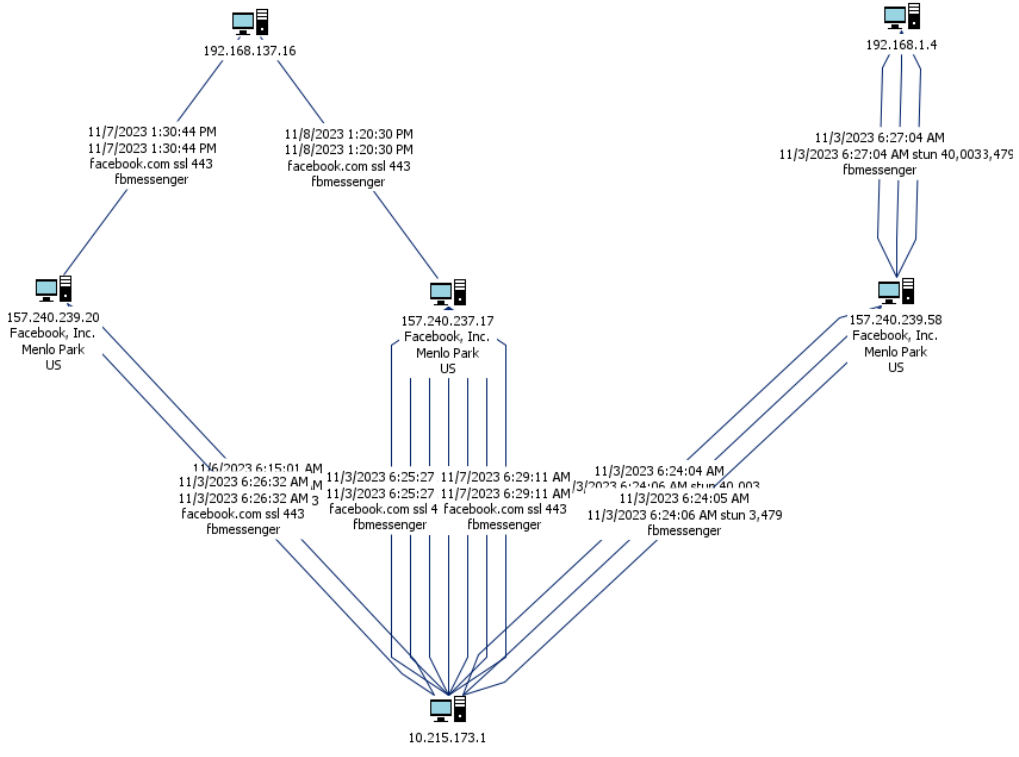
Příklad metadat komunikace

TRANSACTIONTYPE: 11
ISCORRELATED: 0
SERVERIP: 157.240.16.11
SERVERPORT: 443
CLIENTIP: 10.215.173.1
PROTOCOL: ssl
APPLICATION: fbmessenger
DOMAIN: facebook.com
TRANSACTIONSTARTTIME: 11/6/2023 7:06:35 AM
TRANSACTIONENDTIME: 11/6/2023 7:06:35 AM
DATARX: 3,309
DATATX: 345
CERTIFICATEISSUEDTO: facebook.com
EVENTTYPE: 2007
PARTNUMBER: 1
TRANSACTIONID: fb89dda5142f5be0d16bb792dd168446
FILTERID: -1
IFID: 321AAE4A-C3A7-421b-8A9A-5FA9E310FD7E
ASID: 0
ISDATE: Monday
ISUSERPORT: 36760
LIID: 1
ISTRANSPORTTYPE: TCP
FILTERACTION: -1
FILTEROPERATION: -1
FILTERNAME: -1
OFFLINE_SRC_NAME: Offline PCAP
EVENTTYPESTRING: Encrypted Text
TRANSACTIONTYPESTRING: Encrypted Chat Messaging Records
VERSION: 1
PDFILENAME: c:\ISC\DATA_CACHE\72166afb-7f37-45d3-980c-b417314b3626\Target1\PCAPdroid_06_Nov_Nitin.pcap
PDCASEID: 72166afb-7f37-45d3-980c-b417314b3626:#Job_7874280587:#Target1
SESSIONDIRECTION: Unknown
INVESTIGATORID: -1
TARGETCATEGORYID: -1
ISCALLPARTYIP: 0

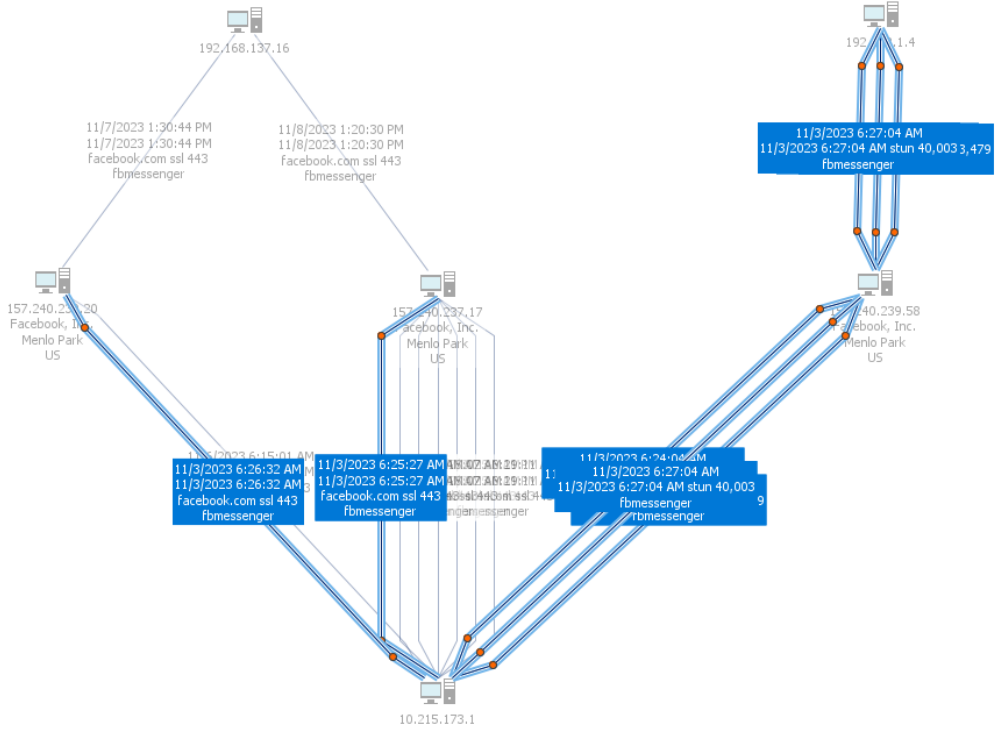
APPLICATION | CLIENTIP

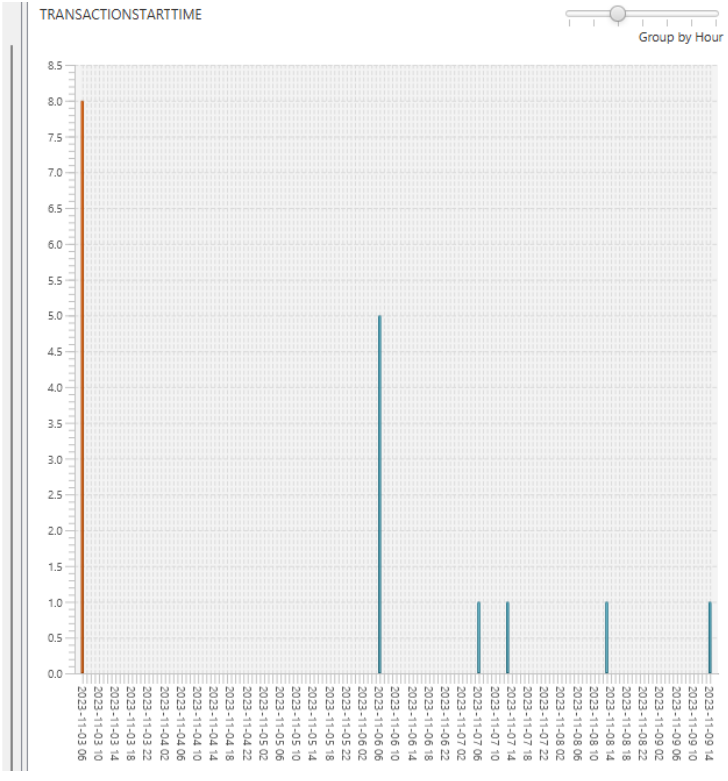
Value	Documents	%
googleads	397	2.81 %
amazon	285	2.02 %
twittersns	258	1.83 %
instagramsns	215	1.52 %
httpothers	197	1.40 %
telegram	166	1.18 %
microsoftteams	146	1.03 %
youtube	145	1.03 %
microsoft	123	0.87 %
google_api_client	122	0.86 %
quic	116	0.82 %
tor	96	0.68 %
amazonwebservices	85	0.60 %
microsoft_365_admin_cen	76	0.54 %
truecaller	58	0.41 %
fb_instagram	55	0.39 %
googleanalytics	52	0.37 %
googlechrome	45	0.32 %
signal	44	0.31 %
uber	38	0.27 %
googlesearch	38	0.27 %
fbmessenger	37	0.26 %
cadkey_tablet_daemon	35	0.25 %
clevertap	32	0.23 %
appsflyer	31	0.22 %
amazon_advertising	30	0.21 %
bharatmatrimony	27	0.19 %
google	26	0.18 %
androidappupdates	26	0.18 %
googlebot	25	0.18 %
linkedinsns	25	0.18 %
crashlytics	25	0.18 %
xiaomi	24	0.17 %
google_fonts	23	0.16 %

Analýza komunikace mezi subjekty

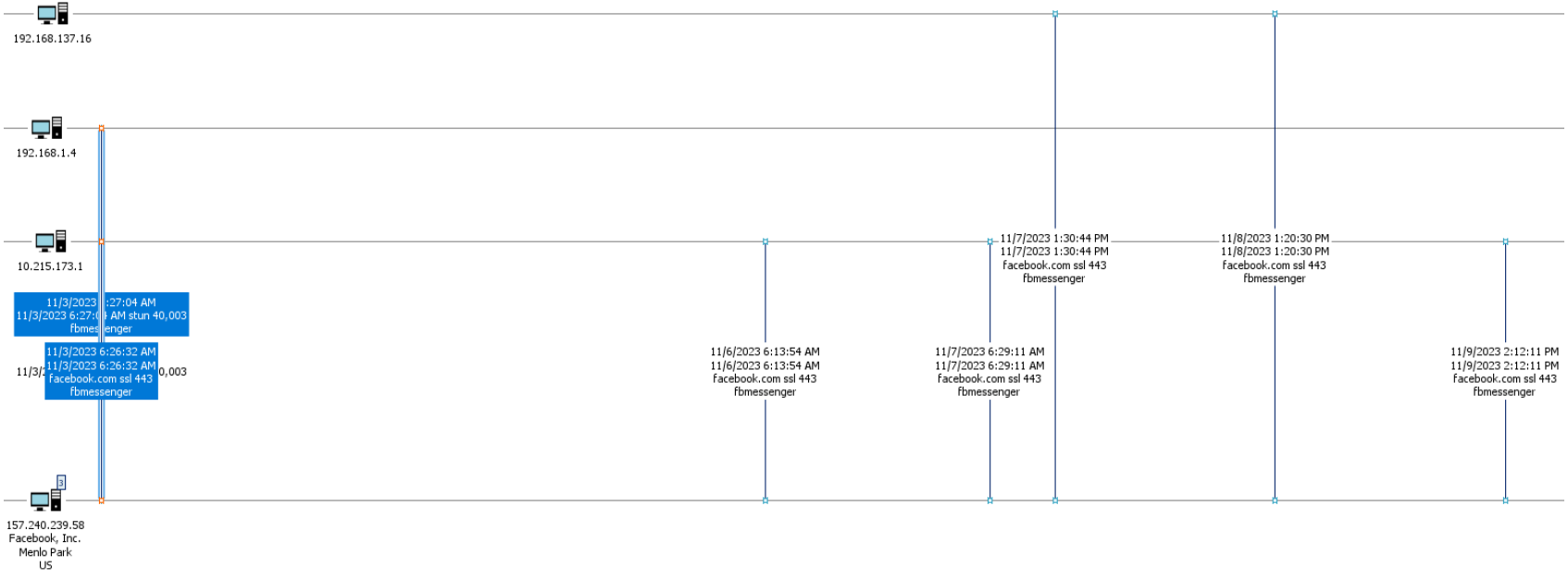


Analýza komunikace mezi subjekty

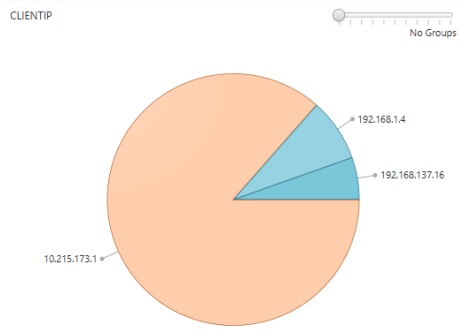


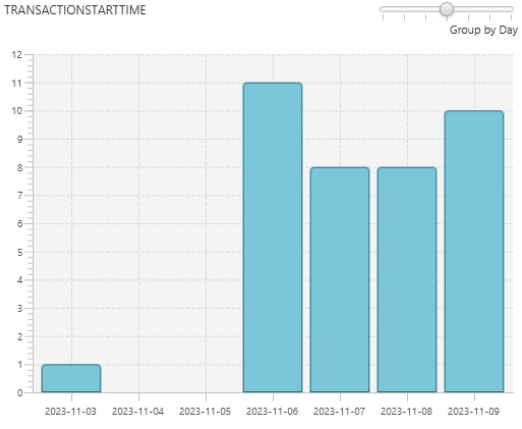


Analýza komunikace mezi subjekty



Profilování subjektu





Value	Documents	%
sslothers	5730	45.13 %
googleservices	1020	8.03 %
facebooksns	959	7.55 %
whatsapp	830	6.54 %
stun	635	5.00 %
unknown	415	3.27 %
googleads	323	2.54 %
amazon	285	2.24 %
twittersns	248	1.95 %
instagramsns	205	1.61 %
httpothers	183	1.44 %
telegram	166	1.31 %
microsoftteams	136	1.07 %
youtube	122	0.96 %
google_api_client	121	0.95 %
tor	96	0.76 %
quic	94	0.74 %
amazonwebservices	85	0.67 %
microsoft_365_admin_center	62	0.49 %
truecaller	58	0.46 %
fb_instagram	53	0.42 %
googleanalytics	52	0.41 %
microsoft	50	0.39 %
signal	44	0.35 %
googlechrome	40	0.32 %
uber	38	0.30 %
googlesearch	38	0.30 %
cadkey_tablet_daemon	35	0.28 %
clevertap	32	0.25 %
fbmessenger	32	0.25 %
appsflyer	31	0.24 %
amazon_advertising	30	0.24 %
bharatmatrimony	27	0.21 %
linkedinsns	25	0.20 %
crashlytics	25	0.20 %
xiaomi	24	0.19 %
googlebot	23	0.18 %

Forenzní analýza

TOVEK

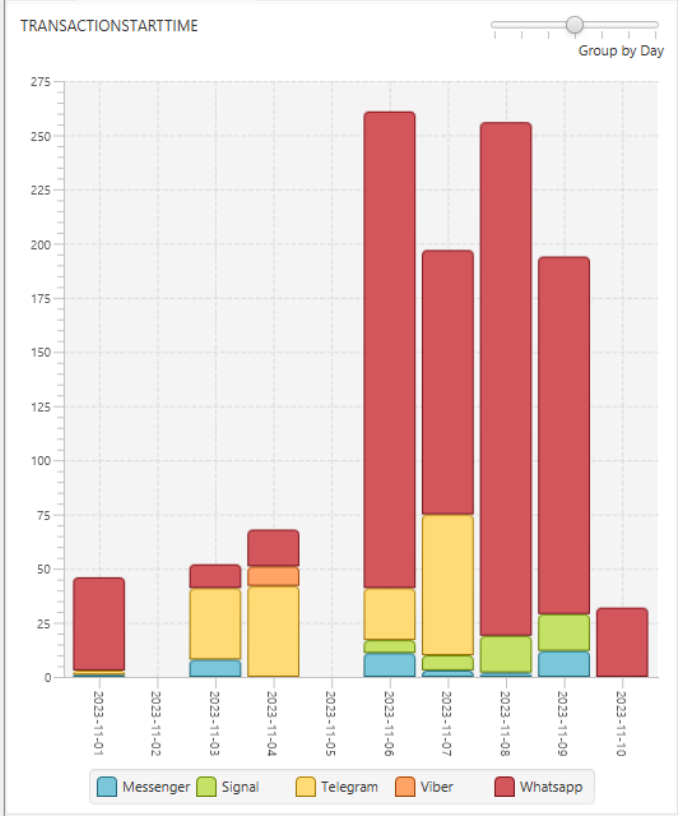
Data ML | IMs

- .any
  - Messenger .word fbmessenger
  - Signal .word signal
  - Telegram .word telegram
  - Viber .word viber
  - Whatsapp .word whatsapp

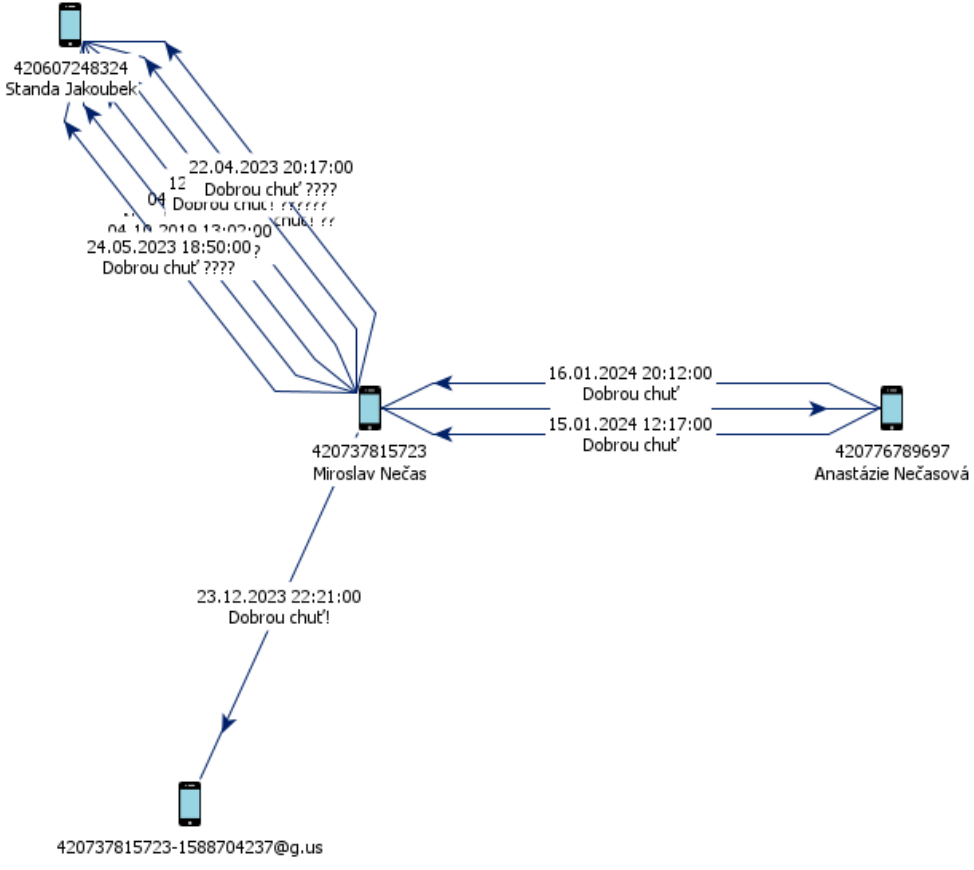
Score	Datum	APPLICATION	TRANSACTIONSTAR...	TRANSACTIONE...	SERVERIP	SERVERPORT	CLIENTIP
45		whatsapp	2023-11-04 17:12:03	2023-11-04 17:12:03	163.70.138.61	443	10.215.173.1
45		whatsapp	2023-11-04 17:30:22	2023-11-04 17:30:22	163.70.138.61	443	10.215.173.1
45		whatsapp	2023-11-04 17:31:57	2023-11-04 17:31:57	163.70.138.61	5222	10.215.173.1
45		whatsapp	2023-11-06 06:17:49	2023-11-06 06:17:50	157.240.237.61	443	10.215.173.1
45		whatsapp	2023-11-06 06:27:54	2023-11-06 06:27:54	157.240.237.61	443	10.215.173.1
45		whatsapp	2023-11-06 06:27:57	2023-11-06 06:28:42	157.240.237.61	443	10.215.173.1
45		whatsapp	2023-11-06 06:33:36	2023-11-06 06:33:36	157.240.237.61	5222	10.215.173.1
45		whatsapp	2023-11-06 07:05:57	2023-11-06 07:05:58	157.240.23.54	443	10.215.173.1
45		whatsapp	2023-11-06 07:06:00	2023-11-06 07:06:00	157.240.23.54	443	10.215.173.1
45		whatsapp	2023-11-06 07:52:32	2023-11-06 07:52:35	157.240.23.54	443	10.215.173.1
45		whatsapp	2023-11-06 07:52:35	2023-11-06 07:52:37	157.240.23.54	443	10.215.173.1
45		whatsapp	2023-11-06 08:39:24	2023-11-06 08:39:29	157.240.23.54	443	10.215.173.1
45		whatsapp	2023-11-06 08:42:10	2023-11-06 08:42:13	157.240.23.54	5222	10.215.173.1
46		whatsapp	2023-11-06 09:45:22	2023-11-06 09:45:22	157.240.16.53	80	10.215.173.1
46		whatsapp	2023-11-06 12:38:36	2023-11-06 12:38:36	157.240.23.54	80	10.215.173.1
46		whatsapp	2023-11-08 06:55:05	2023-11-08 06:55:05	157.240.237.61	80	10.215.173.1
46		whatsapp	2023-11-08 11:58:52	2023-11-08 11:58:52	31.13.66.51	80	10.215.173.1
45		whatsapp	2023-11-09 06:21:38	2023-11-09 06:21:39	157.240.198.61	5222	10.215.173.1
45		whatsapp	2023-11-09 06:24:57	2023-11-09 06:24:57	157.240.198.61	5222	10.215.173.1
45		whatsapp	2023-11-09 06:26:13	2023-11-09 06:26:13	157.240.198.61	5222	10.215.173.1
45		whatsapp	2023-11-09 06:38:42	2023-11-09 06:38:42	157.240.198.61	5222	10.215.173.1
45		whatsapp	2023-11-09 06:38:55	2023-11-09 06:38:55	157.240.198.61	443	10.215.173.1
45		whatsapp	2023-11-09 12:27:38	2023-11-09 12:27:38	157.240.195.54	5222	10.215.173.1
45		whatsapp	2023-11-09 12:27:38	2023-11-09 12:27:39	157.240.195.54	5222	10.215.173.1
45		whatsapp	2023-11-09 12:27:39	2023-11-09 12:27:42	157.240.195.54	5222	10.215.173.1
45		whatsapp	2023-11-09 13:09:22	2023-11-09 13:09:46	157.240.195.54	443	10.215.173.1
45		whatsapp	2023-11-09 13:15:31	2023-11-09 13:15:51	157.240.195.54	443	10.215.173.1

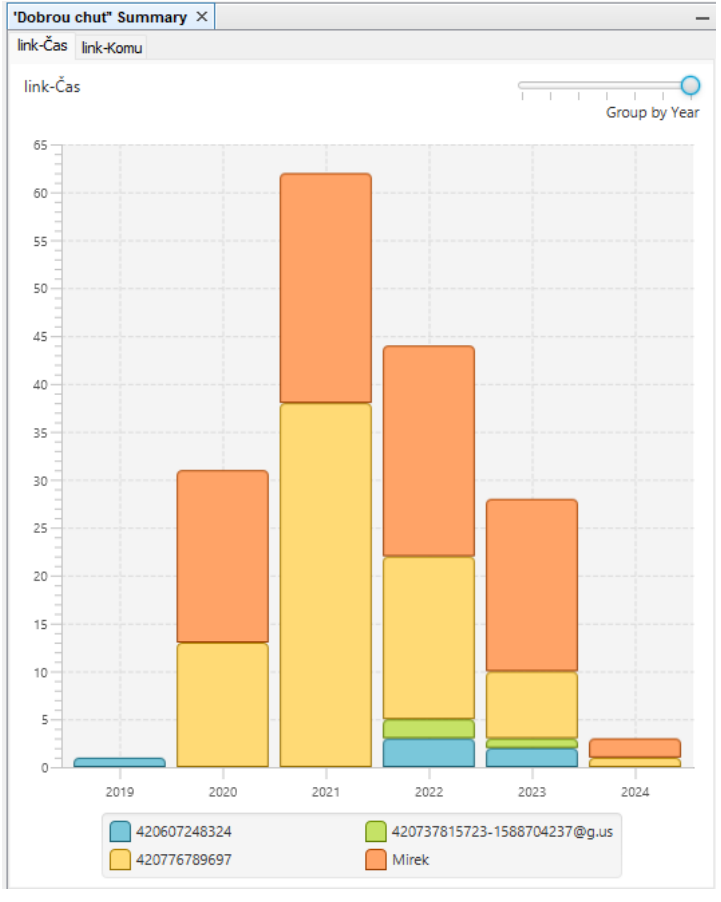
'IMs' Summary

CLIENTIP | TRANSACTIONSTARTTIME | APPLICATION



Data z mobilního telefonu





Využití AI

- Kombinace ML a expertních pravidel:
  - Zpřesnění IOC oproti JA3 otiskům
  - Identifikace zdrojů kybernetických hrozeb
  - Identifikace dalších IP adres / subjektů ve skupině komunikujících osob

- Předpoklad
  - Nasazení na úrovni podniku / operátora
  - Výpočetní výkon (v případě použití ML)
  - Legálnost takového počínání

Otázky a odpovědi

TOVEK

- Analýza komunikace mezi zájmovými subjekty
  - Jaké aplikace pro komunikaci používají?
  - V jakém čase a z jakých míst komunikují
  - Jaké používají IP adresy / zařízení
- Profilování určitého subjektu / IP adresy
  - Jaké aplikace používá?
  - V jakém čase a z jakých míst komunikuje
- Forenzní analýza zachyceného provozu
  - Identifikace zájmové komunikace na základě aplikace, času…
  - … pro výběr a podrobnou analýzu dat z dalších zdrojů

TOVEK

Děkuji vám za pozornost!

Miroslav Nečas

necas@tovek.cz

find ▸
understand ▸
use ▸