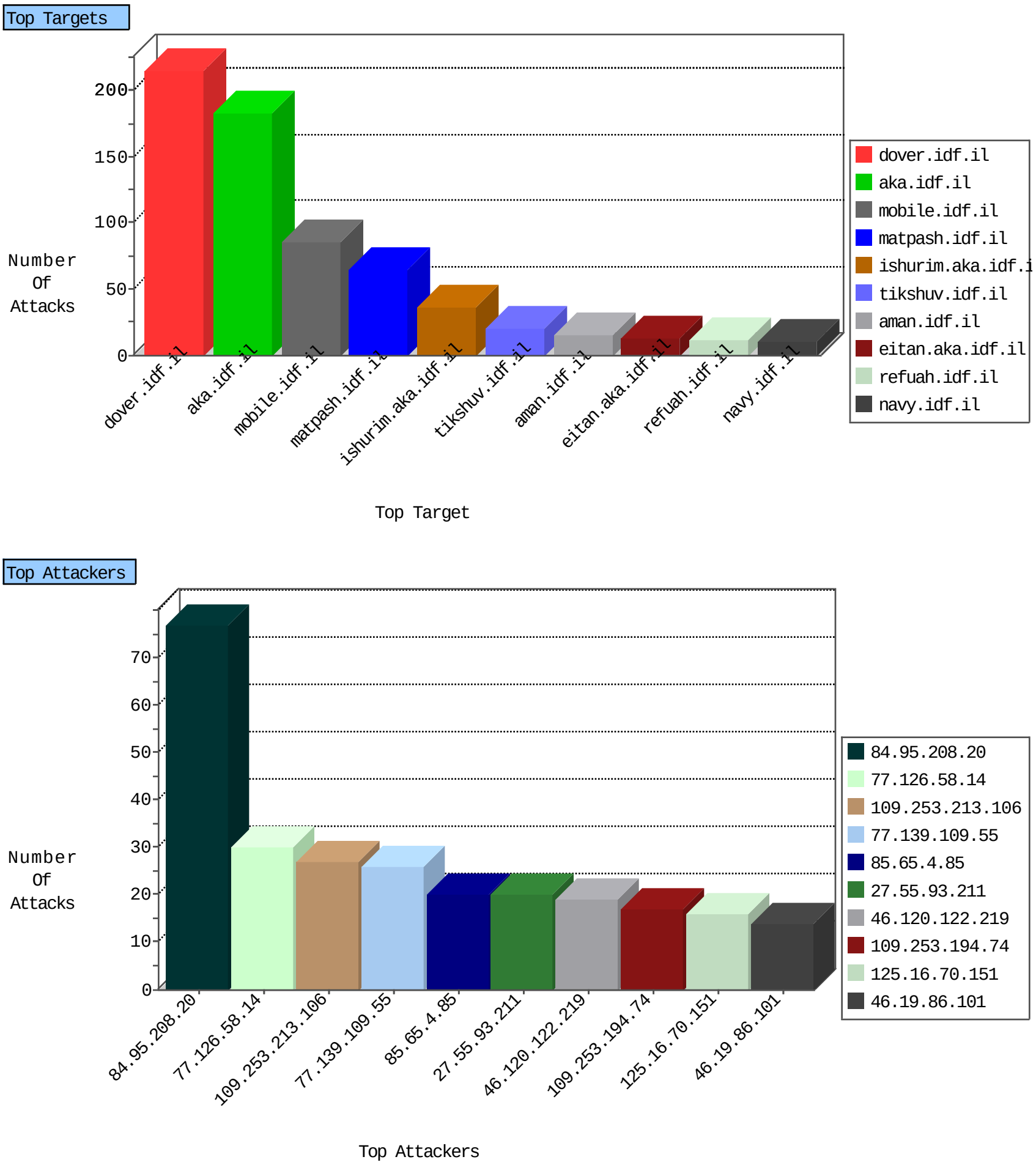
10-01-2016-20:04:07 to 10-01-2016-21:04:07

IDF Under Attack Daily Report



10-01-2016-20:04:07 to 10-01-2016-21:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.60.48.25	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
192.69.89.173	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1

10-01-2016-20:04:07 to 10-01-2016-21:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
125.208.24.2	China	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	3

10-01-2016-20:04:07 to 10-01-2016-21:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
161.202.163.70	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
113.175.240.251	147.237.77.178	Vietnam	e.matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
88.133.35.158	147.237.72.167	Germany	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
52.187.42.85	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.72.209.112	147.237.77.235	China	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
161.202.163.70	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
161.202.163.70	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
161.202.163.70	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
93.174.164.92	147.237.77.243	Romania	mobile.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
62.210.243.100	147.237.8.50	France	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
40.84.189.118	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
161.202.163.70	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
161.202.163.70	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1

10-01-2016-20:04:07 to 10-01-2016-21:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
27.55.93.211	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
85.65.4.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
125.16.70.151	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
213.6.79.110	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
109.253.194.74	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.188	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.213.106	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
109.253.213.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.13.23	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
2.55.156.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
67.167.18.101	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
109.66.122.43	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
77.139.109.55	France	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.75.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
100.92.116.241		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.176	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.139.109.55	France	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
109.253.192.169	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
185.120.126.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.253.192.169	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
62.16.70.208	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
109.253.213.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.18.18.239	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
77.139.109.55	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.81.224.50	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
62.16.70.208	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.64.111.150	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
176.13.11.205	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
217.132.51.26	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
131.253.25.245	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.120.122.219	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	4
46.19.86.176	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
176.13.249.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.15.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.253.194.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.120.122.219	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
157.55.39.196	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
214.14.214.69	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
109.253.213.106	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
185.24.207.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.230.84.64	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
87.197.164.92	Slovakia	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
46.19.86.101	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
80.246.139.155	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.3.147.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.169	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

10-01-2016-20:04:07 to 10-01-2016-21:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	74
109.253.132.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
77.138.14.213	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
62.82.98.250	Spain	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.183.39.16	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.183.39.16	Block	2
77.138.131.44	France	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
58.11.68.185	Thailand	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
88.15.241.70	Spain	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
79.176.97.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.12	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1765	Block	1
2.53.167.246	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
176.13.22.43	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
83.215.180.178	Austria	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
77.139.70.32	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
95.86.111.15	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
79.183.39.16	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.65.135	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9740-he/refuah.aspx	Block	1
5.29.197.241	Israel	147.237.72.166	aka.idf.il	Unknown Parameter asm in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
192.243.55.130	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
77.139.104.93	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/miluim/about.aspx	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
109.67.244.34	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
77.127.245.147	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.85.140	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEW in www.aka.idf.il/main/sachar/	None	1
207.46.13.10	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
77.139.109.55	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/kamlar/	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 66.102.9.8	Block	1
79.183.39.16	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
46.19.85.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.68.7.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/g	Block	1
79.71.153.206	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
2.53.34.226	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
82.81.224.50	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

10-01-2016-20:04:07 to 10-01-2016-21:04:07