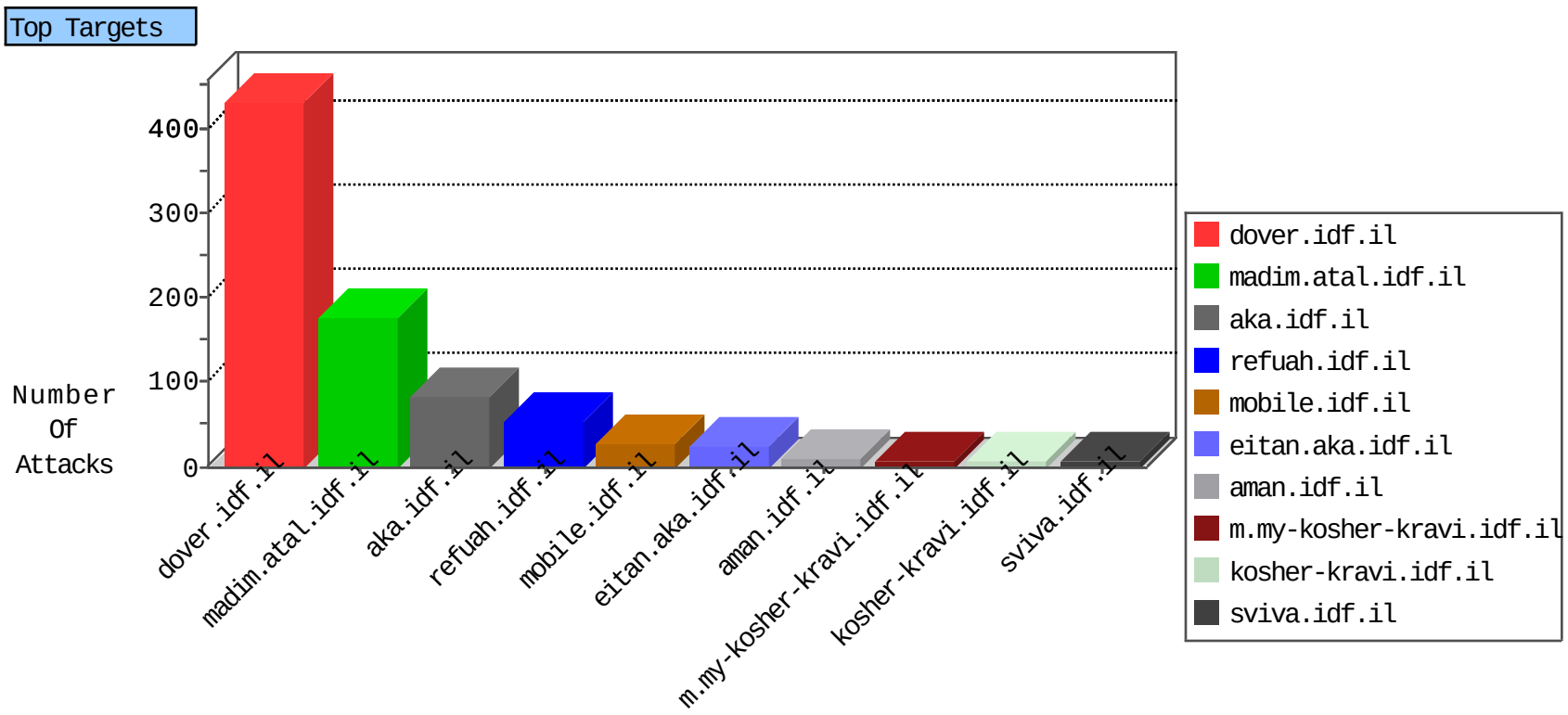
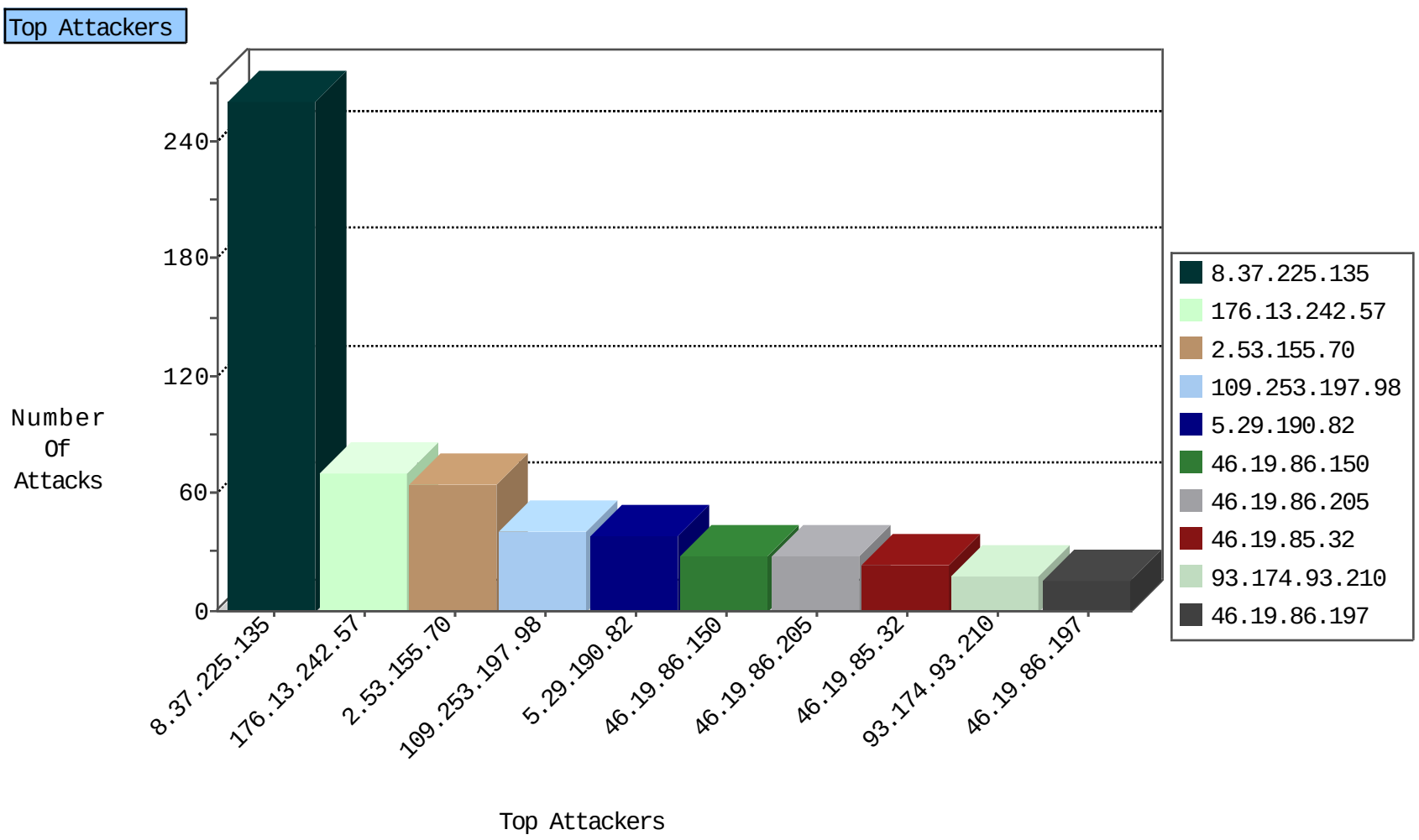
10-04-2016-14:04:01 to 10-04-2016-15:04:01

IDF Under Attack
Daily Report





10-04-2016-14:04:01 to 10-04-2016-15:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.225.135	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
8.37.225.135	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
93.174.93.210	Netherlands	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
93.174.93.210	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
93.174.93.210	Netherlands	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
71.6.216.38	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	1

10-04-2016-14:04:01 to 10-04-2016-15:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-04-2016-14:04:01 to 10-04-2016-15:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 4096	1
208.100.26.228	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
199.96.83.13	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
112.84.116.175	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
77.125.52.231	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
66.240.213.93	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
54.147.50.220	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 3072	1
208.100.26.228	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
199.96.83.13	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.243.100	147.237.76.39	France	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

10-04-2016-14:04:01 to 10-04-2016-15:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	253
5.29.190.82	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
46.19.86.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.19.86.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
77.127.72.71	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.32.208.187	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.86.197	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
95.35.169.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.142.201.158	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.102.195.71	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.84.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.228.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.197.98	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
109.253.197.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.197.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.253.197.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.193.32	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
109.253.197.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
109.253.197.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.149.198	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
95.82.40.73	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.46.41.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.174.93.210	Netherlands	147.237.0.15	kosher-kravi.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
109.253.197.98	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.197.98	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
79.176.7.59	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
213.57.232.98	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.57	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
109.253.140.210	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.174.93.210	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
100.92.182.121		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.197	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
80.179.104.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.66.166.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
213.57.52.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.53.157.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
93.174.93.210	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.53.149.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.58	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.142.201.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.229.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
213.57.232.98	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
85.65.24.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

10-04-2016-14:04:01 to 10-04-2016-15:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.242.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	70
2.53.155.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
46.19.86.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	28
85.64.157.242	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.64.157.242	Block	12
95.35.169.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.34.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.143.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.146.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.33.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.139.75.123	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	2
79.176.7.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
2.55.183.0	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.86.176	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	1
207.182.140.210	United States	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/	Block	1
84.111.226.251	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	1
5.29.190.82	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
176.13.228.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in 147.237.72.166/main/giyus/general.aspx	Block	1
213.8.114.33	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1
5.102.195.71	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/69851.pdf	Block	1
46.135.109.0	Czech Republic	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
213.57.232.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.71.32.190	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.67	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9043-he/refuah.aspx	Block	1
185.120.126.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/rec.asp	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/63076.pdf	Block	1
89.18.128.106	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.69.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8941-he/refuah.aspx	Block	1
37.26.147.167	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
185.143.41.10		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1

10-04-2016-14:04:01 to 10-04-2016-15:04:01