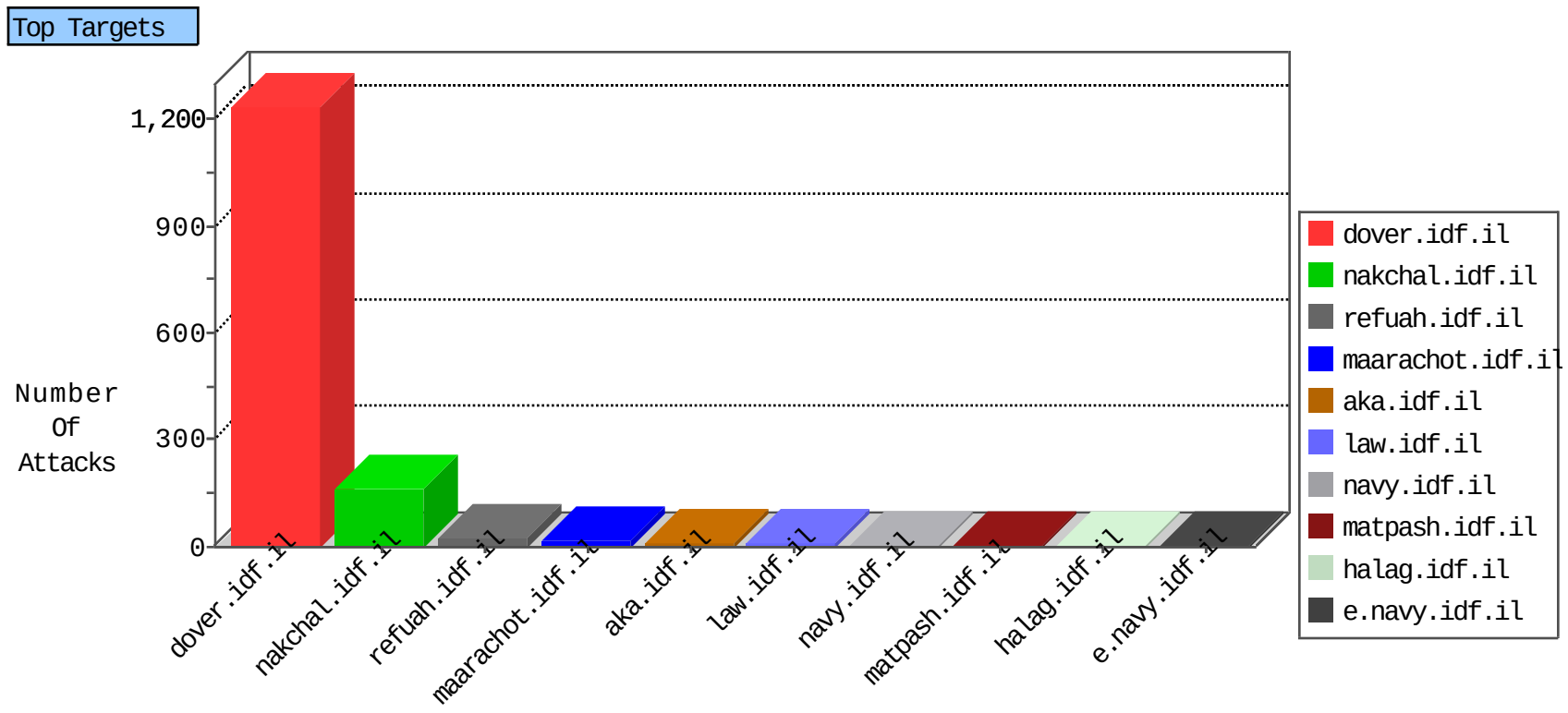
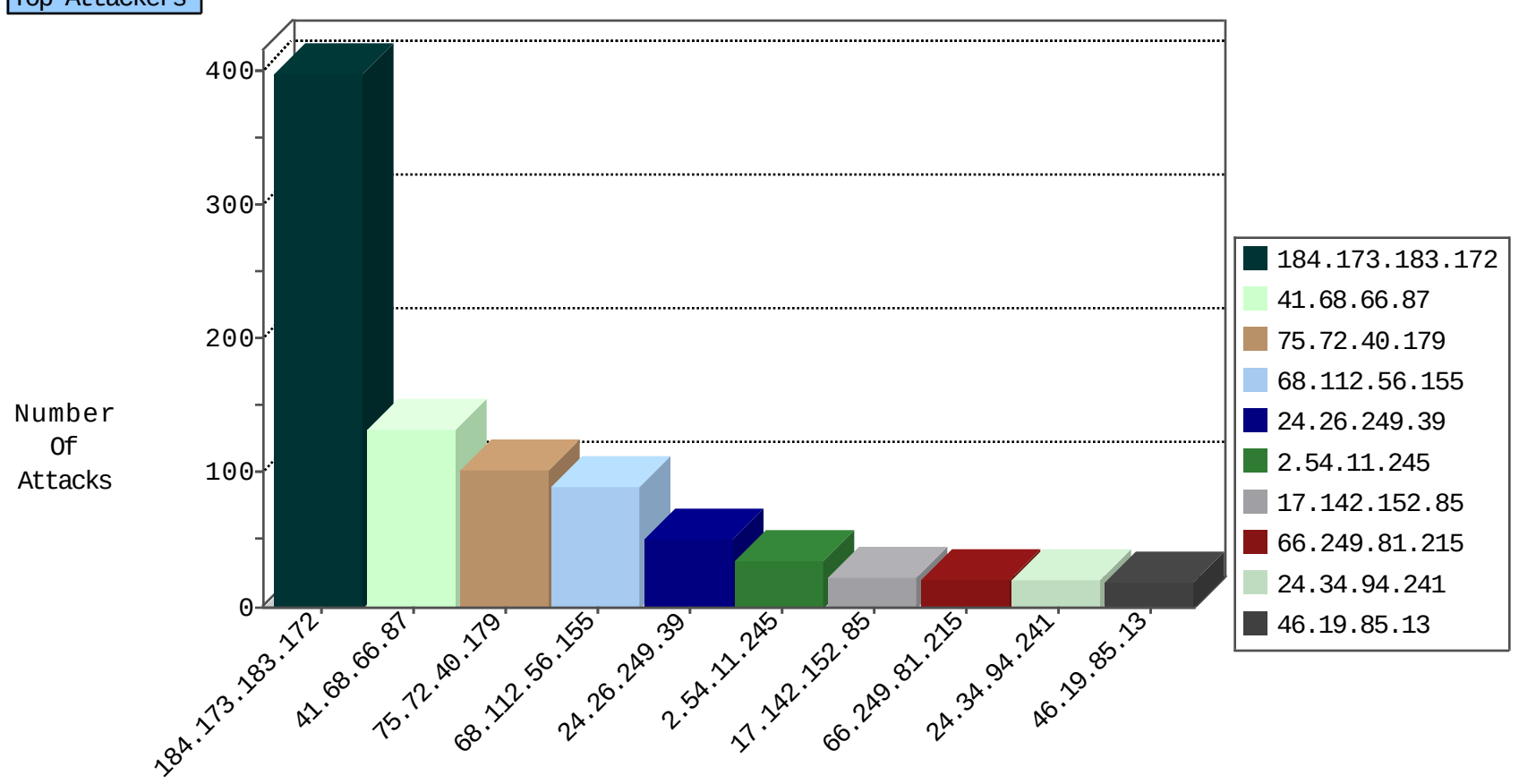
04-20-2015-03:03:07 to 04-20-2015-04:03:07

IDF Under Attack
04-20-2015-03:03:07

Top Targets



Top Attackers



04-20-2015-03:03:07 to 04-20-2015-04:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.142	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	392
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	219
220.181.108.185	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	212
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	149
82.145.218.1	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.240.236.119	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1

04-20-2015-03:03:07 to 04-20-2015-04:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	397
89.139.173.79	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
188.138.9.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
184.173.183.172	United States	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1

04-20-2015-03:03:07 to 04-20-2015-04:03:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.67.41	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	10
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
104.167.117.197		147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
81.200.91.2	Russian Federation	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.67	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.158.162.40	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
146.148.93.253		147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 2048	1
104.167.117.197		147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
81.200.91.2	Russian Federation	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.65	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
213.182.43.222	France	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.65	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
146.148.93.253		147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 4096	1
146.148.93.253		147.237.77.234	halag.idf.il	ET SCAN NMAP -f -sS	1

04-20-2015-03:03:07 to 04-20-2015-04:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
41.68.66.87	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	133
75.72.40.179	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	101
68.112.56.155	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	90
24.26.249.39	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
2.54.11.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
17.142.152.85	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
24.34.94.241	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
46.19.85.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
17.142.152.110	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
17.142.152.68	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
17.142.152.72	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.19.85.106	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	monitor	12
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
17.142.152.81	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
17.142.152.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
17.142.152.132	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
17.142.152.94	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.81.215	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
69.116.248.156	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
17.142.152.111	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
69.123.36.190	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.83.194	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
75.94.70.61	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
208.69.40.107	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
17.142.152.86	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
192.99.170.80	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.35	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
17.142.145.3	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
218.218.18.173	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
72.76.37.83	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
72.185.240.148	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
173.55.97.91	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
75.67.21.62	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.174.166.140	Turkey	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
59.167.118.165	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
173.76.92.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.64.129.128	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.144.127	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2

04-20-2015-03:03:07 to 04-20-2015-04:03:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
178.137.85.64	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	3
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
157.55.39.31	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.31	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/facebook.com/tzahalonline	Block	1
180.76.4.170	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
84.108.65.245	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/history/6day.stm	Block	1
157.55.39.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info11.stm	Block	1
37.115.187.54	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
207.46.13.124	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
94.136.40.100	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.65.186	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on 147.237.77.74//	Block	1
157.55.39.97	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.stm	Block	1
54.80.166.99	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
95.173.190.4	Turkey	147.237.77.234	halag.idf.il	Illegal HTTP Version	Block	1
66.249.67.33	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
173.10.238.251	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
66.249.64.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/rights/asp/faq.asp	None	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
75.72.40.179	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter itemid in www.aka.idf.il/kamlar/gallery/showpicture.asp	None	1

04-20-2015-03:03:07 to 04-20-2015-04:03:07