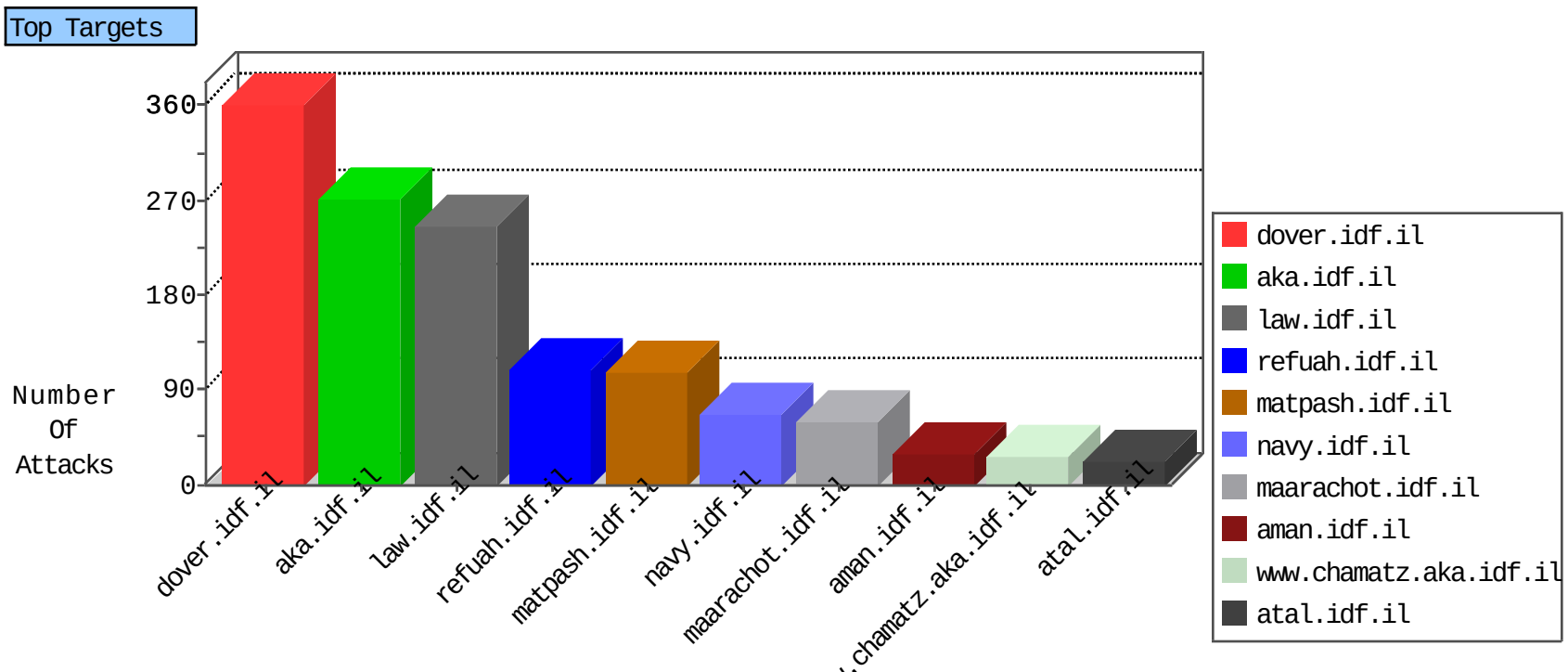
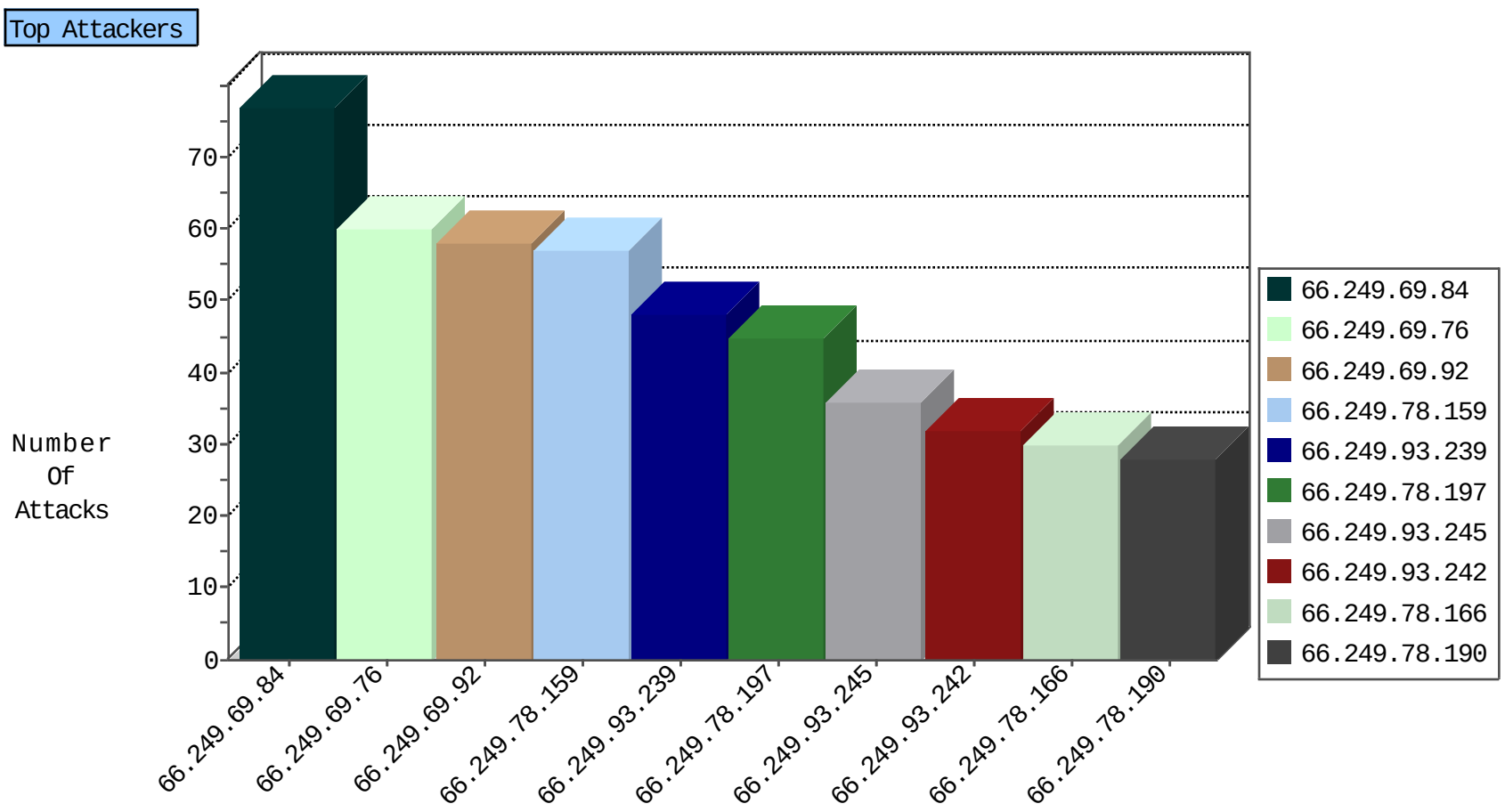
04-04-2015-15:03:04 to 04-04-2015-16:03:04

IDF Under Attack
04-04-2015-15:03:04

Top Targets



Top Attackers



04-04-2015-15:03:04 to 04-04-2015-16:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.69.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	77
66.249.69.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	59
66.249.69.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	58
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	57
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	48
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	45
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	36
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	32
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	30
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	28
66.249.67.157	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	26
66.249.64.118	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	26
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	24
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	23
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	23
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	22
66.249.64.114	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	19
66.249.75.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	18
66.249.67.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	16
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	16
66.249.75.68	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	15
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	14
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	13
66.249.67.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.75.60	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.67.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.67.5	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.64.110	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
66.249.67.13	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.67.26	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	9
66.249.78.45	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	8
66.249.93.200	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	7
66.249.78.191	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	6
66.249.81.145	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	6
66.249.78.242	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.249.78.38	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	6
66.249.64.45	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	5
66.249.67.74	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.78.141	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	5
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	5
66.249.75.103	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	5
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.78.31	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	4
66.249.81.140	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	4
66.249.67.29	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
66.249.78.184	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	4
66.249.75.9	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	4
66.249.93.208	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	4

04-04-2015-15:03:04 to 04-04-2015-16:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.108.103.193	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
213.57.165.45	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
197.37.202.27	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
218.6.132.45	China	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	2
46.19.85.97	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.14	e.orchot.idf.il	DVRep_P-N_40-59	Permit	1
84.109.235.156	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
87.69.191.205	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-04-2015-15:03:04 to 04-04-2015-16:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	26
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
122.228.207.76	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.6.132.45	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
122.228.207.76	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
188.166.37.194	Russian Federation	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.130		147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
151.11.201.3	Italy	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 2048	1
151.11.201.3	Italy	147.237.77.74	law.idf.il	ET SCAN NMAP -f -sS	1
122.228.207.76	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
218.6.132.45	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
122.228.207.76	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
114.255.149.210	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.130		147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
151.11.201.3	Italy	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.151	China	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

04-04-2015-15:03:04 to 04-04-2015-16:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
109.253.134.182	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.139.192	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
109.253.135.34	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.137.211	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.151.105	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
93.186.31.81	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
41.186.56.187	Rwanda	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	7
109.253.137.59	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.201.83.50	Ukraine	147.237.77.121	e.navy.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	6
203.127.96.249	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
157.55.39.6	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
37.247.36.119	Netherlands	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	6
109.253.149.175	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
2.52.6.249	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
2.52.6.249	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
2.52.6.249	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
2.52.39.73	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
46.19.85.55	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
109.253.158.227	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
2.52.39.73	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
2.52.39.73	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	4
46.19.85.55	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
93.186.31.97	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
93.186.31.113	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
5.102.254.83	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
188.120.148.180	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
188.120.148.180	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
31.186.228.27	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.86.178	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
5.102.254.83	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
85.65.106.155	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
31.186.228.67	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
188.120.148.149	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
31.186.228.91	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
2.187.253.17	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
109.253.149.68	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
192.99.19.38	Canada	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.93	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
2.187.253.17	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
188.120.148.180	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	2
31.186.228.23	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
37.26.146.199	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
5.9.97.92	Germany	147.237.76.202	e.halag.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
85.65.54.135	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.121.145.22	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
176.12.145.210	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
202.153.70.151	Australia	147.237.77.216	dover.idf.il	header rejection pattern found in request	Header Rejection	monitor	1
2.54.153.209	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
80.179.96.90	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
185.32.177.106	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

04-04-2015-15:03:04 to 04-04-2015-16:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.57.165.45	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	9
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
78.46.203.72	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/webresource.axd	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
77.125.80.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.125.80.106	Block	2
149.78.10.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
84.108.103.193	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
50.198.201.34	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
188.165.15.23	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.172.176.52	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
77.125.80.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wepdwukmty5nzc4oti0nq9kfgjmd2qwamypzbycagmpzbycagcpzbycagmpzbycagepd2qwah4hb25jbgljaww5avnlbmrfbwfpbcgnumvzb3vyy2vzl1nlcnzpy2vzl3dztwf0zxjpywxzlmfzbxgvu2v0rw1hawwnlcqoj21hawxcb3gnkswkkcdzcevyck1hawwnkswkkcd0ehrfbwfpbccplnzhbhvllcqoj2nwae1haw5fy29udgvude1haw5bcmvhx2ltz1nlbmrfbwfpbccplcqoj2nwae1haw5fy29udgvude1haw5bcmvhx2ltz0xvywqnksk7zgrijvlxxenuh9kx7vc2ozcxnl0j+tpe7hdjfhyxsdy6nq==/	Block	1
2.52.170.174	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.78.202.69	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	1
84.109.213.123	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
50.198.201.34	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
93.172.182.30	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
5.29.20.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
155.254.245.94		147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
84.110.55.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
52.4.217.48	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/shared/usercontrols/headerupper/	Block	1
202.153.70.151	Australia	147.237.77.216	dover.idf.il	Distributed eMail Hoarding	Block	1
96.45.107.121	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.177.160.234	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
46.120.220.167	Israel	147.237.72.166	aka.idf.il	Unknown Parameter mouduleToGoTo in www.aka.idf.il/main/giyus/login.aspx	None	1
84.111.38.20	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
203.133.169.157	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/journal.stm	Block	1
109.253.149.198	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.179.203.60	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
46.121.247.56	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19831-he/kkkkkkk=d9eccbcakkkkkkk_d9eccbca	Block	1
85.65.54.135	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
207.46.13.2	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1

04-04-2015-15:03:04 to 04-04-2015-16:03:04