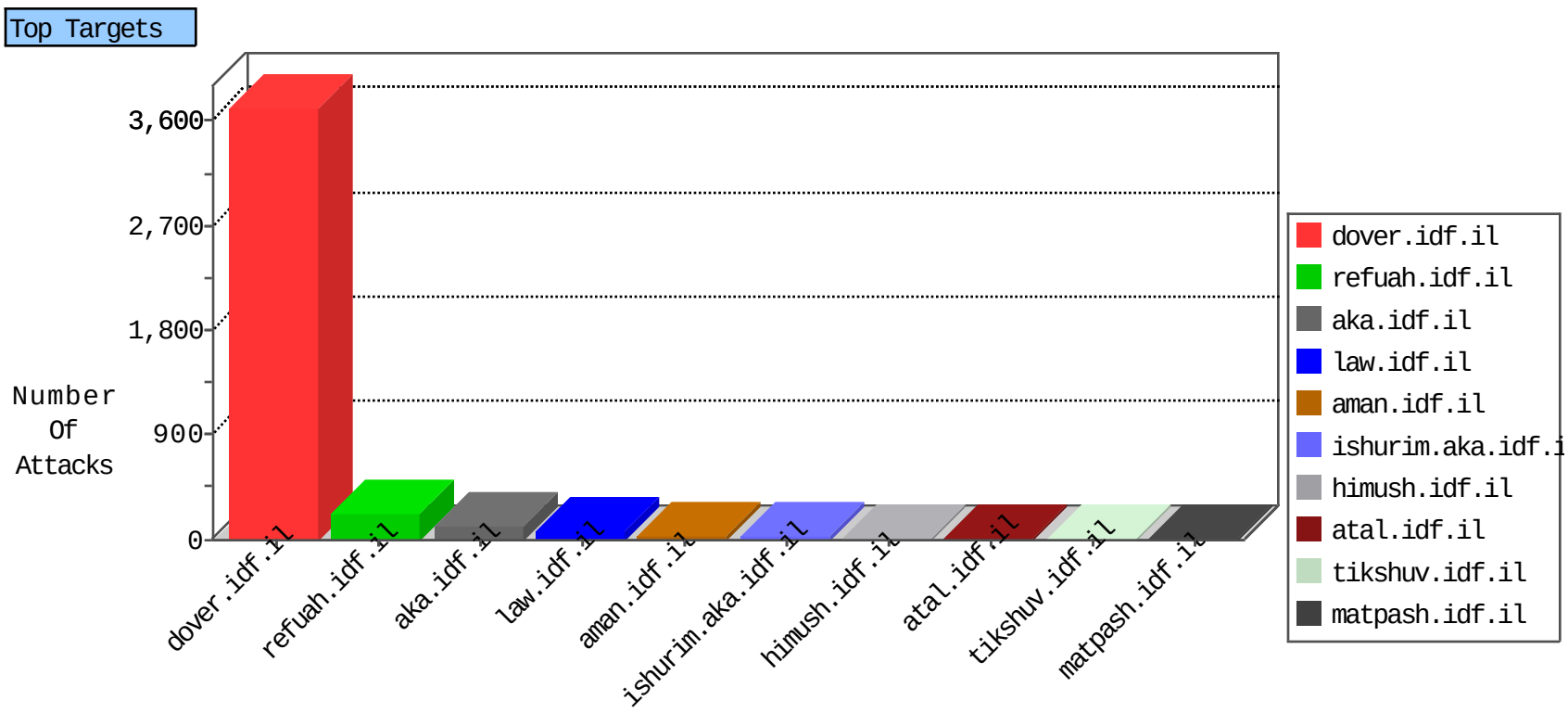
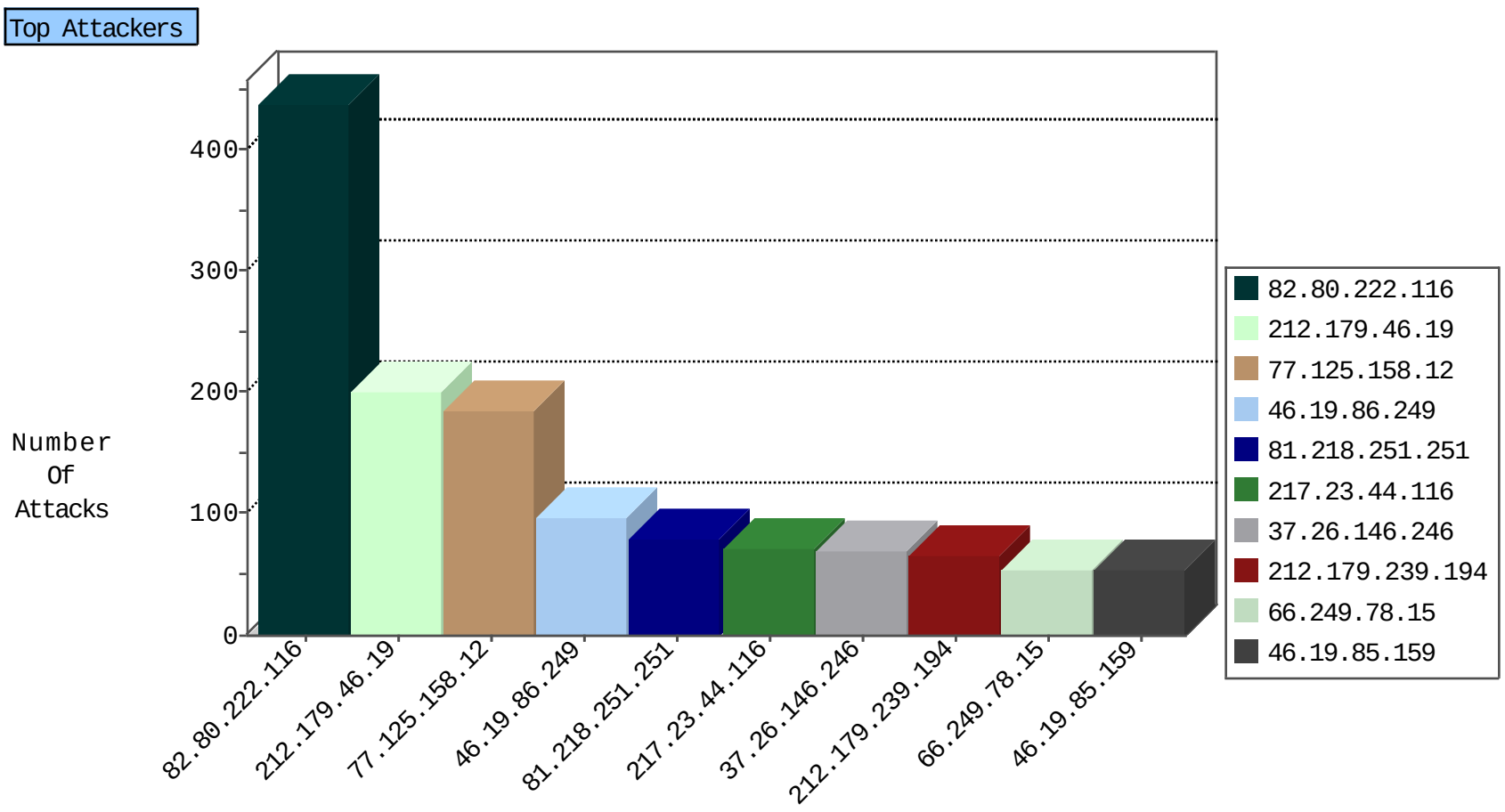
05-05-2015-09:03:01 to 05-05-2015-10:03:01

IDF Under Attack
05-05-2015-09:03:01

Top Targets



Top Attackers



05-05-2015-09:03:01 to 05-05-2015-10:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
82.166.184.140	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2666
2.54.189.147	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
82.145.219.46	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	17
82.145.209.218	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
37.26.147.165	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
109.253.159.113	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
109.253.142.103	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.117.78.159	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
124.232.142.220	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.60	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

05-05-2015-09:03:01 to 05-05-2015-10:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.125.158.12	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
81.218.251.252	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.131	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
66.240.236.119	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	2
212.199.244.112	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
82.102.141.249	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.120.17.94	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
79.182.18.50	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
84.109.212.111	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
58.146.173.200	Singapore	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
80.246.138.127	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.131	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
80.246.138.233	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.190	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1
66.240.236.119	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.216	dover.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
46.19.86.71	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1

05-05-2015-09:03:01 to 05-05-2015-10:03:01

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	54
79.179.180.125	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
176.31.126.12	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
106.39.95.194	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.251.125	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
80.230.38.196	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.185.90	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
201.239.118.143	Chile	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.67.108	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	1
194.0.91.188	Ukraine	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
194.0.91.188	Ukraine	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
185.32.177.208	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
123.138.215.145	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
93.172.14.8	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.138.210	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.244.112	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
79.183.167.204	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.39.125	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
194.0.91.188	Ukraine	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
2.52.191.106	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
192.114.3.241	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

05-05-2015-09:03:01 to 05-05-2015-10:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.80.222.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	426
212.179.46.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	196
77.125.158.12	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	174
46.19.86.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	97
81.218.251.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	80
217.23.44.116	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	71
37.26.146.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	69
46.19.85.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
212.179.239.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
82.80.231.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
109.253.141.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
93.172.56.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
109.253.131.97	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
109.253.137.187	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
176.12.147.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
80.246.133.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
176.12.142.103	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
86.111.145.210	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
80.179.223.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
2.54.47.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
81.218.126.226	Israel	147.237.77.74	law.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	24
212.179.61.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
2.54.164.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
109.253.130.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.136.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
2.54.135.211	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
66.249.64.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
212.179.185.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
94.188.146.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
66.249.64.76	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
212.235.98.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
124.188.116.60	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
2.54.52.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
212.199.185.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
199.203.240.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
46.19.85.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13

05-05-2015-09:03:01 to 05-05-2015-10:03:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
82.80.222.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	12
157.55.39.4	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
2.54.54.85	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.95.131.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.204	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.204	Block	2
157.55.39.7	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.7	Block	2
192.95.16.191	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
93.172.164.169	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
212.179.46.19	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
176.12.145.79	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip.storage/files/4/	Block	1
46.19.85.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
212.179.61.120	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
87.69.97.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/login	Block	1
79.181.52.94	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.116.83.2	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1613-15490-he/dover.aspx	Block	1
103.247.9.13	Indonesia	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.64.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/mobile/	Block	1
2.54.190.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.179.46.19	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 212.179.46.19	Block	1
185.32.178.208	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1202-1.stm	Block	1
66.249.64.245	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17032-he/dover.aspx	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.69.250.236	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
46.29.89.50	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
216.218.206.66	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
79.183.189.201	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.91	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
109.66.173.124	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mazi.idf.il	Block	1
5.29.23.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.179.46.19	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.179.46.19	Block	1
84.108.217.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
77.125.158.12	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
185.61.138.244		147.237.77.233	atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.67.76	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
89.138.194.123	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
58.146.173.200	Singapore	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.179.10.4	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
208.113.184.223	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
176.12.140.223	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
66.249.64.88	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1

05-05-2015-09:03:01 to 05-05-2015-10:03:01