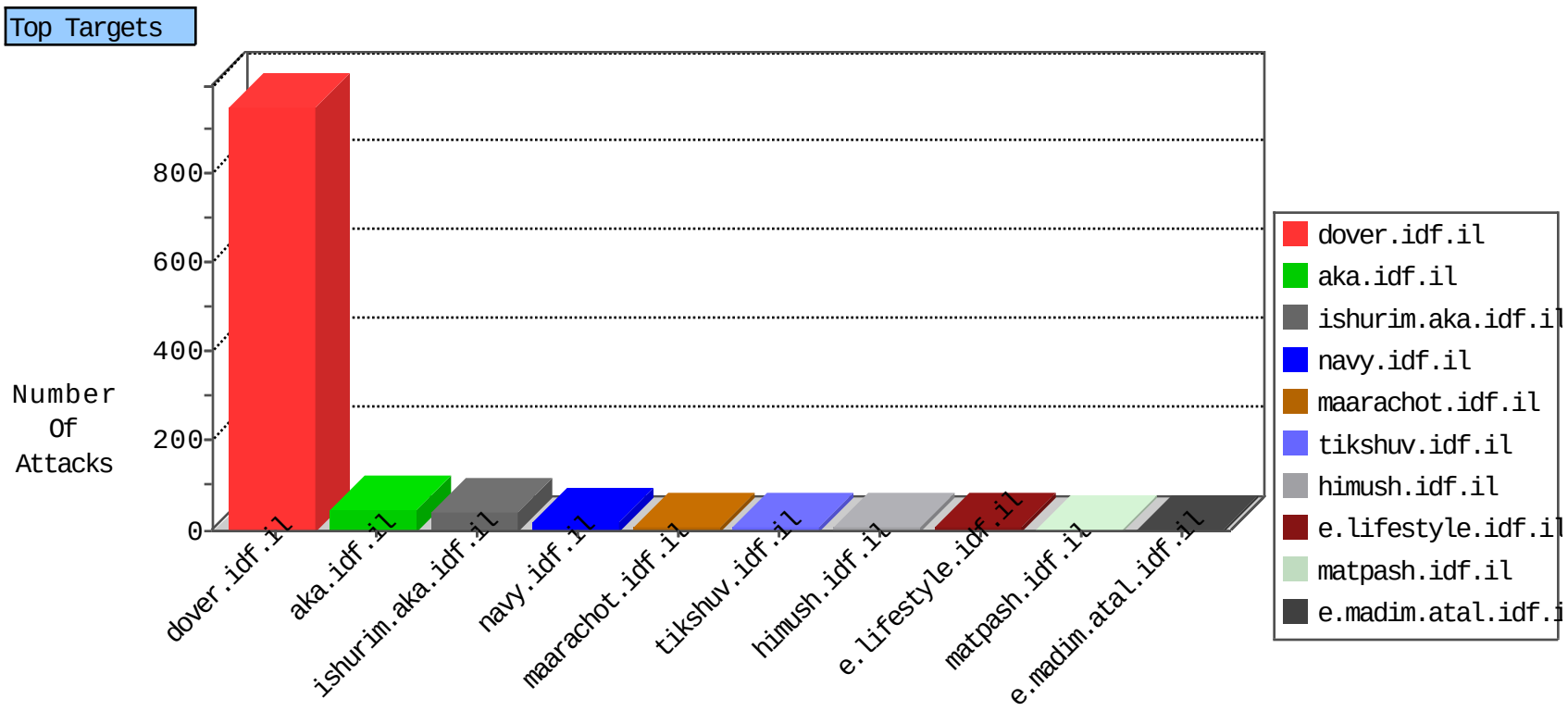
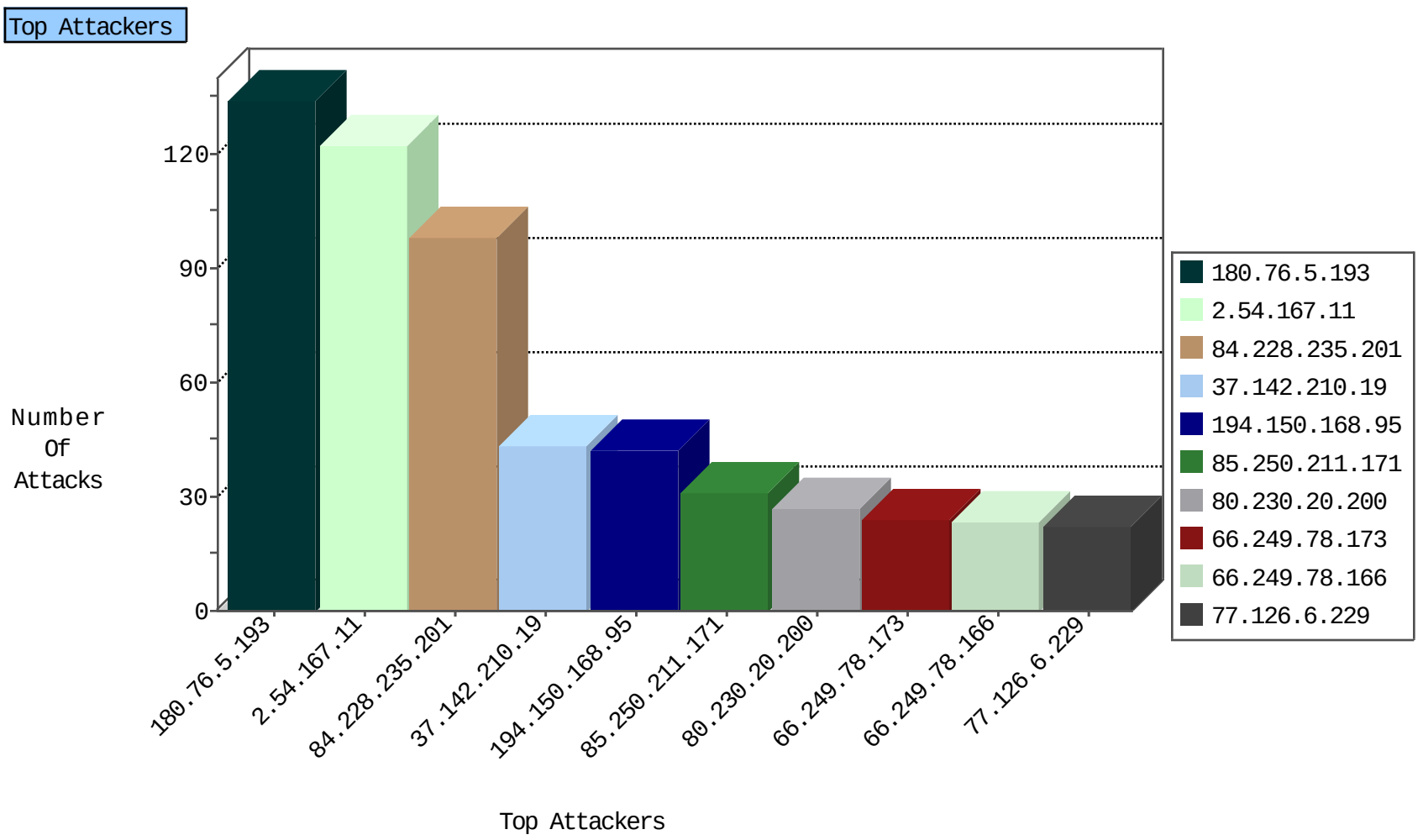
05-09-2015-09:03:05 to 05-09-2015-10:03:05

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

Top Targets



Top Attackers



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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
37.142.210.19	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	576
66.249.67.172	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	85
84.110.109.241	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
46.19.86.136	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	68
220.181.108.88	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	15
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
194.177.16.3	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
68.116.5.134	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	134
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	22
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
195.142.179.50	Turkey	147.237.77.170	maarachot.idf.il	12373: HTTP: WordPress admin Login	Block	4
73.46.239.4	United States	147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	Block	1
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
72.1.242.79	United States	147.237.76.34	yohalan.idf.il	DVRep_P-N_40-59	Permit	1
66.240.192.138	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
82.166.118.168	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
72.1.242.79	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_P-N_40-59	Permit	1
66.240.192.138	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
46.166.186.237	Netherlands	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
72.1.242.79	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	1
66.240.192.138	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
72.1.242.79	United States	147.237.76.177	ncore.idf.il	DVRep_P-N_40-59	Permit	1
66.240.192.138	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
72.1.242.79	United States	147.237.76.30	himush.idf.il	DVRep_P-N_40-59	Permit	1
66.240.192.138	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1

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

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
79.176.63.1	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
202.112.113.26	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
110.55.118.159	Philippines	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.112.113.26	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
72.1.242.79	United States	147.237.76.177	ncore.idf.il	GPL SCAN superscan echo	1
72.1.242.79	United States	147.237.76.38	e.e.meitav.idf.il	GPL SCAN superscan echo	1
175.136.197.37	Malaysia	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 4096	1
72.1.242.79	United States	147.237.76.30	himush.idf.il	GPL SCAN superscan echo	1
221.235.189.244	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
175.136.197.37	Malaysia	147.237.76.30	himush.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.67	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
221.235.189.244	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
175.136.197.37	Malaysia	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.235.189.244	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
116.121.137.2	Korea, Republic of	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.244	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.59.33.61	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
202.112.113.26	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
110.55.118.159	Philippines	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.64	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
110.55.118.159	Philippines	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.64	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.112.113.26	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
202.112.113.26	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
72.1.242.79	United States	147.237.76.42	refuah.idf.il	GPL SCAN superscan echo	1
178.19.107.114	Poland	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
72.1.242.79	United States	147.237.76.34	yohalan.idf.il	GPL SCAN superscan echo	1
221.235.189.244	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
175.136.197.37	Malaysia	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 2048	1
221.235.189.244	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
175.136.197.37	Malaysia	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.66	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.244	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
116.121.137.2	Korea, Republic of	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.244	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
116.121.137.2	Korea, Republic of	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.244	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.59.33.61	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -f -sS	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.54.167.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	122
84.228.235.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	98
194.150.168.95	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
85.250.211.171	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
80.230.20.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
77.126.6.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
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
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
80.246.133.80	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
220.255.1.135	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
94.230.86.212	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
46.19.86.210	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.64.178	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
46.116.170.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.19.85.101	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
79.178.130.77	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.182.56.130	Israel	147.237.76.86	navy.idf.il	First packet isn't SYN	drop	drop	6
46.120.210.10	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
84.95.57.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.120.210.10	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
108.204.28.72	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
220.255.1.77	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.86.210	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
87.68.87.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
173.63.189.80	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
82.205.70.214	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
213.244.119.129	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.0	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
31.168.164.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.64.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.18.51.73	Russian Federation	147.237.8.24	e.lifestyle.idf	Geo-location inbound enforcement	Geo-location enforcement	drop	4
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.120.210.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.183.59.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.23	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.139	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
50.139.255.137	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.117.112.247	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
109.253.147.136	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	3
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
162.243.81.121	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 162.243.81.121	Block	2
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/shalishut/site/resources/controls/general.aspx	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2000/september/21.stm	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.109.194.182	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
162.243.81.121	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
2.54.20.116	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
74.82.47.3	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/foia/foia.stm	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/klali.aspx	Block	1
2.54.63.55	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.66	Block	1
79.181.167.38	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/newsflash/www.ynet.co.il	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in www.aka.idf.il/lomdim/forum/asp/showforum.asp	None	1
144.76.62.165	Germany	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/	Block	1
5.135.158.101	France	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/patzar	Block	1
80.246.130.237	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.73	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1086-13341-en/dover.aspx forcerecrawl: 0	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.173	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en/matpash.aspx	Block	1
5.241.77.83	Sweden	147.237.76.86	navy.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unknown Parameter sig2 in www.aka.idf.il/main/giyus/general.aspx	None	1
80.246.133.96	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1

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