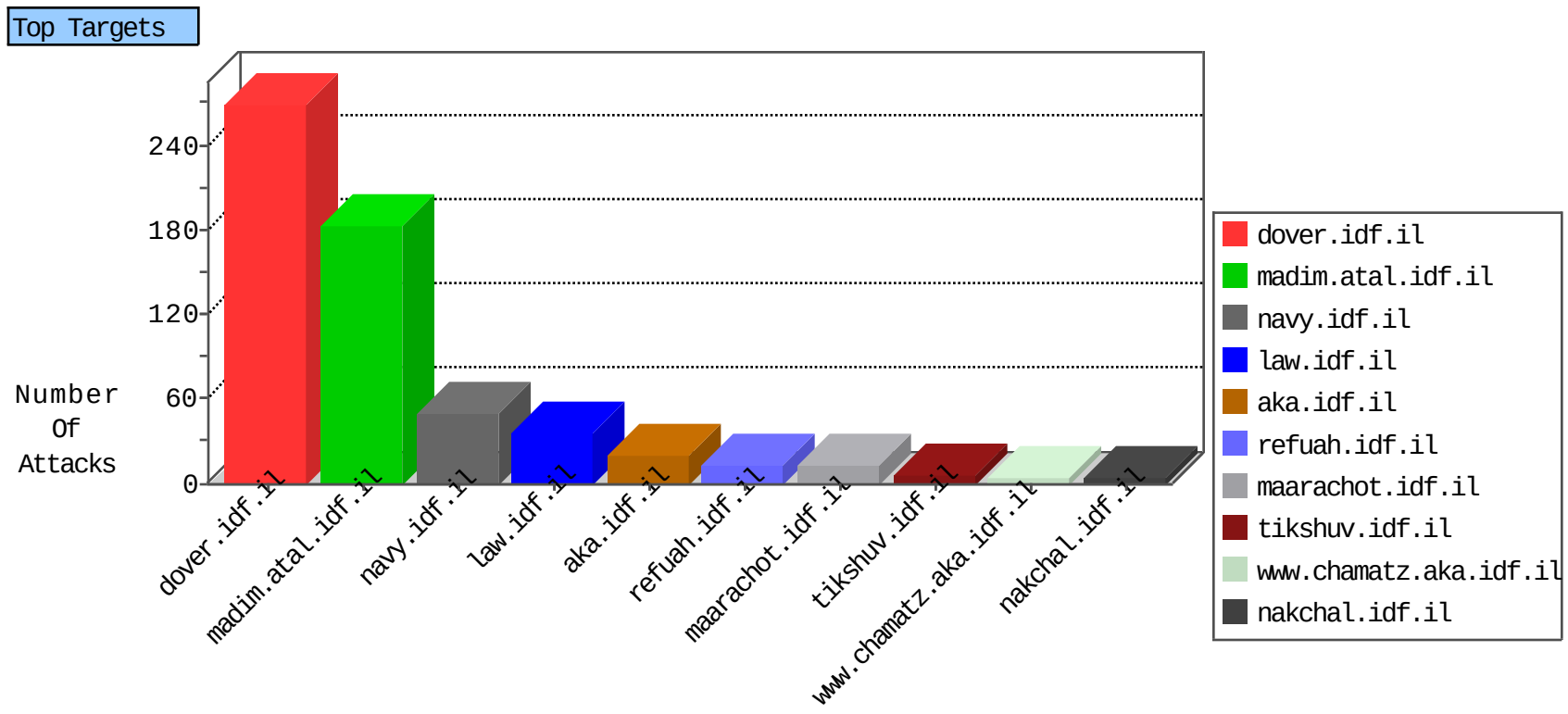
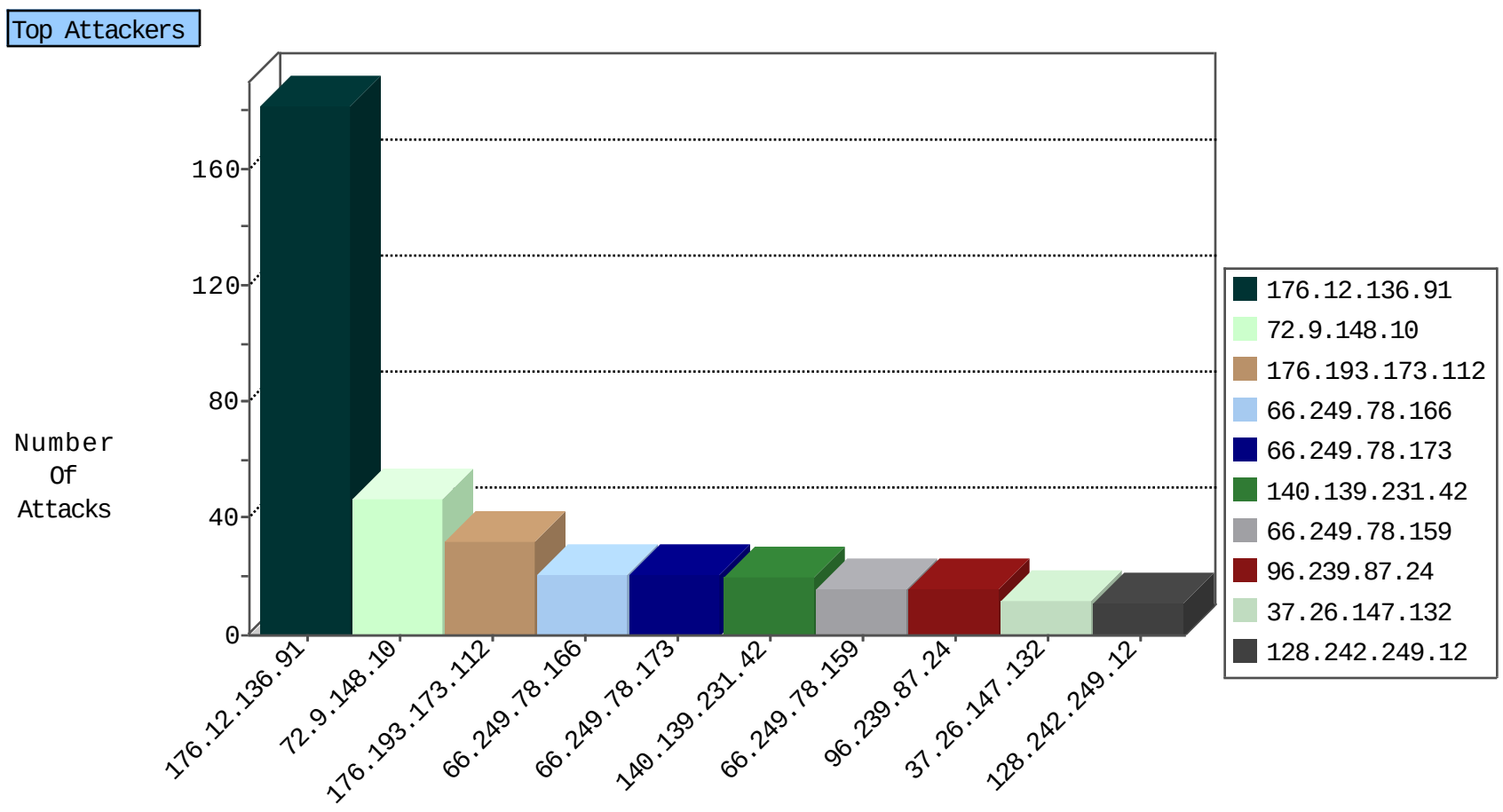
05-09-2015-00:03:03 to 05-09-2015-01:03:03

IDF Under Attack
05-09-2015-00:03:03

Top Targets



Top Attackers



05-09-2015-00:03:03 to 05-09-2015-01:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.179	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	118
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	7
71.6.165.200	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

05-09-2015-00:03:03 to 05-09-2015-01:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	8
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
66.240.192.138	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	2
85.25.103.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	2
198.20.70.114	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.72.14	dover.idf.il(old)	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
188.138.9.50	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
80.246.136.71	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.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
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	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
71.6.135.131	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.42	refuah.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	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.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
93.120.27.62	Romania	147.237.77.216	dover.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	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.45	e.eitan.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
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1

05-09-2015-00:03:03 to 05-09-2015-01:03:03

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
66.249.67.29	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
218.77.79.43	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
120.85.130.148	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
210.61.150.154	Taiwan	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
109.92.114.145		147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.130		147.237.0.200	m4u.idf.il	ET SCAN NMAP -f -sS	1
188.138.9.51	Germany	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
81.200.91.2	Russian Federation	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
121.88.5.177	Korea, Republic of	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
121.88.5.177	Korea, Republic of	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
121.88.5.177	Korea, Republic of	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
121.46.0.125	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
120.85.130.148	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
210.61.150.154	Taiwan	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
109.186.55.105	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
210.61.150.154	Taiwan	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -f -sS	1
104.128.144.130		147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
188.138.9.51	Germany	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
94.131.14.10	Russian Federation	147.237.72.156	aman.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
125.129.97.249	Korea, Republic of	147.237.0.34	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
81.200.91.2	Russian Federation	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
121.88.5.177	Korea, Republic of	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
121.88.5.177	Korea, Republic of	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
121.46.0.125	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
218.77.79.43	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
121.46.0.125	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1

05-09-2015-00:03:03 to 05-09-2015-01:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
176.193.173.112	Russian Federation	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	32
140.139.231.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
96.239.87.24	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
5.102.254.215	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
84.228.194.231	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
88.75.121.105	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
50.1.104.135	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
192.116.128.90	Israel	147.237.77.170	maarachot.idf.il	First packet isn't SYN	drop	drop	7
46.19.86.115	Israel	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
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
31.210.187.135	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
80.212.27.194	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
178.152.188.73	Qatar	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.26.147.132	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
213.67.203.117	Sweden	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.26.147.132	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
24.47.78.27	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
128.242.249.12	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.186.185.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
84.228.165.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.154.63	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.26.147.132	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
2.54.154.63	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.26.147.132	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.117.44.150	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
37.231.147.168	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.8.11.119	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.26	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.117.44.150	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
173.76.25.100	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.63.35.241	Bahrain	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
31.210.186.237	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
37.26.147.132	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
5.102.254.215	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.116.126.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.75.215.116	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
68.4.48.252	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
199.119.124.38	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
142.161.95.163	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.86.34	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
94.159.238.233	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
208.73.200.8	United States	147.237.77.216	dover.idf.il	header rejection pattern found in request	Header Rejection	monitor	1
66.249.81.222	Israel	147.237.76.31	nakchal.idf.il	directory traversal overflow	Directory Traversal	monitor	1
109.253.143.219	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
2.92.221.198	Russian Federation	147.237.77.74	law.idf.il	'Referer' header length exceeded maximum allowed length	HTTP Format Sizes	monitor	1
66.249.64.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
37.75.215.116	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.136.91	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.136.91	Block	181
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	47
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	12
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	12
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	4
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	4
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	4
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	4
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	2
46.117.55.30	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	2
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	2
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	1
180.76.5.65	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/120403-2.stm	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
208.73.200.8	United States	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
66.249.64.199	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
157.55.39.141	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/894-7860-he	Block	1
46.19.85.138	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
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
188.65.113.241	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
77.125.2.150	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl103 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	1
208.73.200.8	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
66.249.64.238	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.162	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.91.86.5	Czech Republic	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
208.73.200.8	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
66.249.67.206	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1681-he/refuah.aspx	Block	1
176.12.136.91	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	1
52.6.169.50	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jump.stm	Block	1
66.249.79.193	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/eitan/listpage/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	1
207.46.13.137	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
85.250.62.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.75.58	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	1
66.249.81.222	Israel	147.237.76.31	nakchal.idf.il	URL is Above Root Directory www.nakhal.idf.il/../favicon.ico	Block	1
208.73.200.8	United States	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	1
96.47.41.22	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
37.202.99.169	Jordan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//aman	Block	1