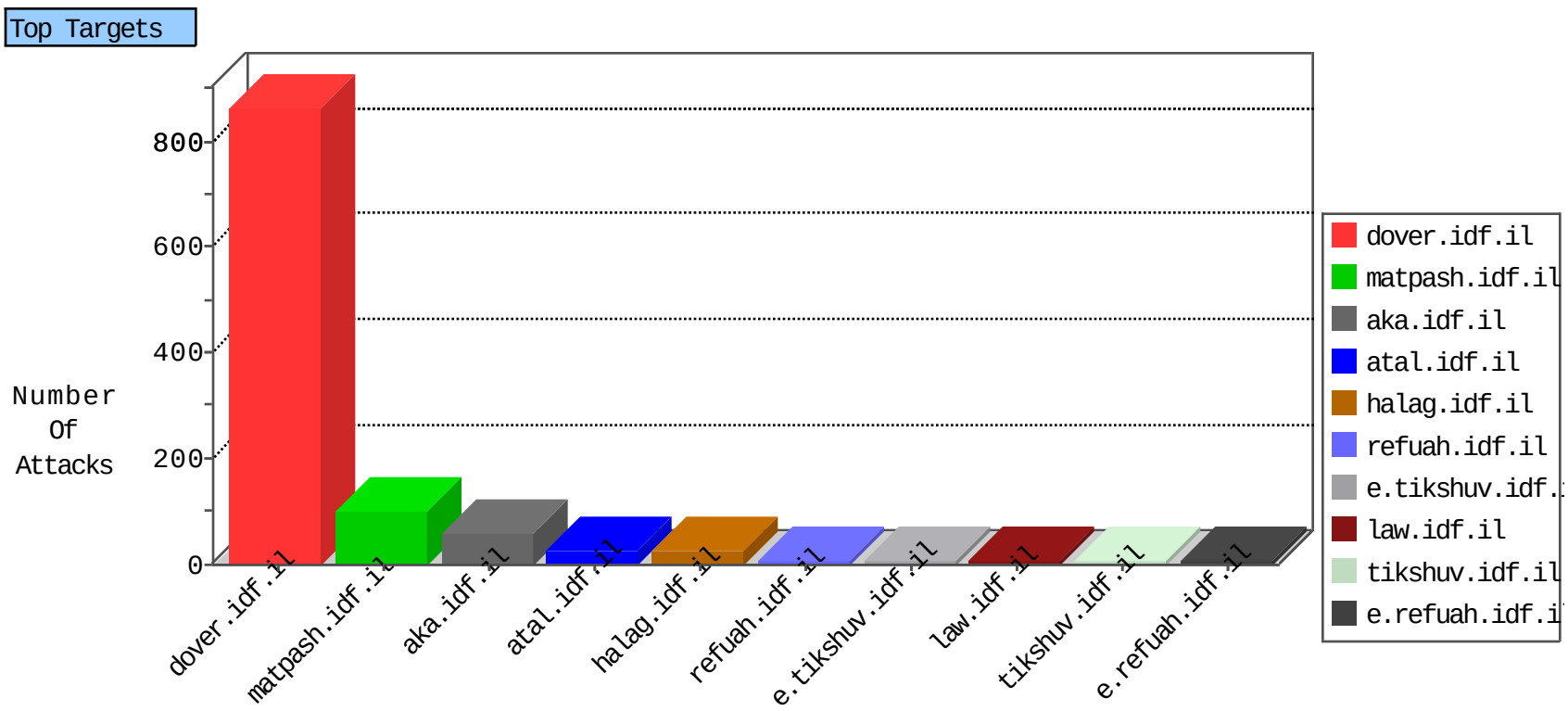
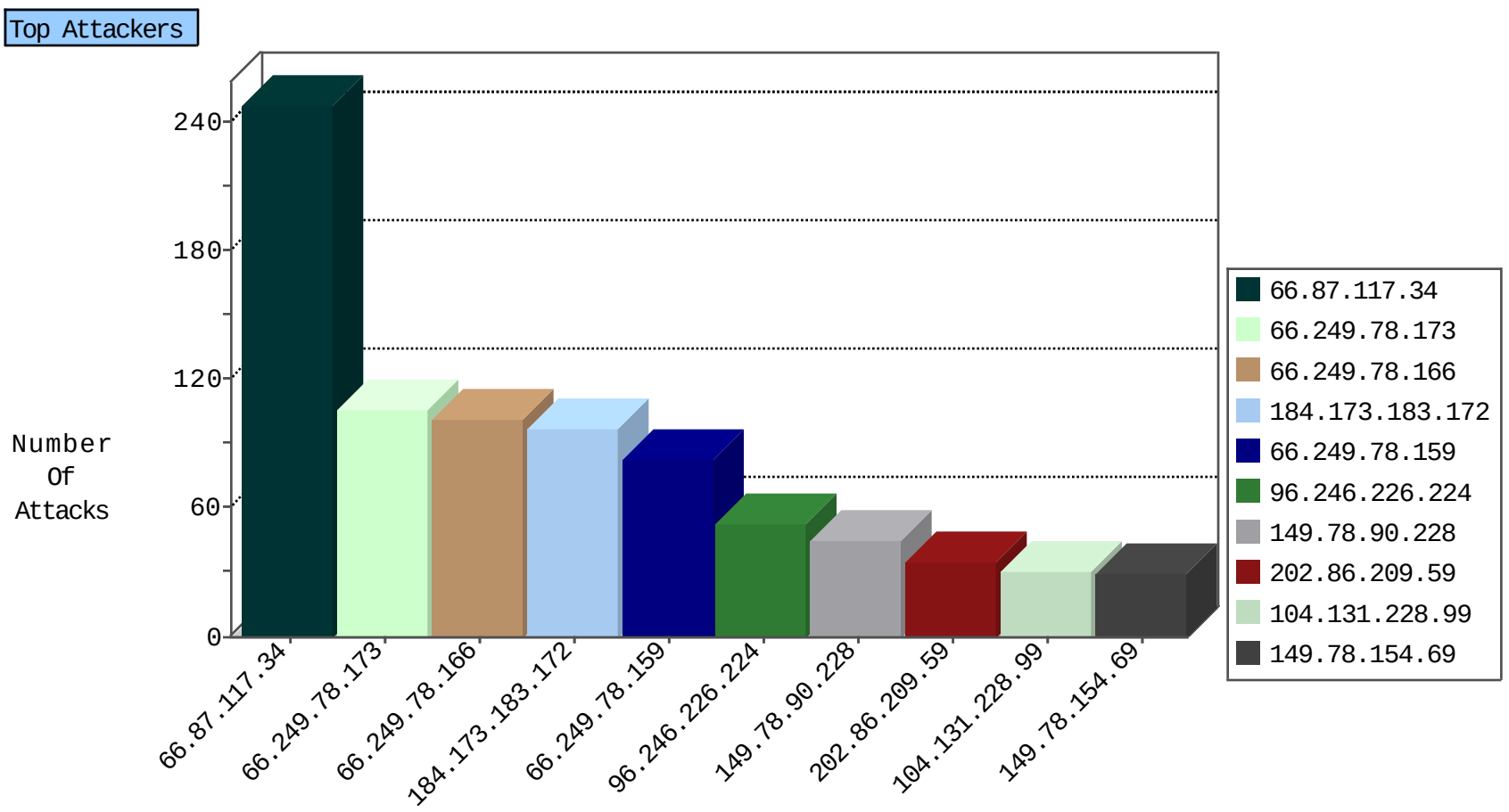
05-04-2015-06:03:04 to 05-04-2015-07:03:04

IDF Under Attack
05-04-2015-06:03:04

Top Targets



Top Attackers



05-04-2015-06:03:04 to 05-04-2015-07:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	288
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	42
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5

05-04-2015-06:03:04 to 05-04-2015-07:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	97
188.138.9.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.14	e.orchot.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	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.170	maarachot.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
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.34	yohalan.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	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
149.78.90.228	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.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
66.240.236.119	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.200	m4u.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	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.199	e.nakchal.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

05-04-2015-06:03:04 to 05-04-2015-07:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.110.35.13	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
109.65.122.143	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.165	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
106.39.95.194	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
221.143.48.200	Korea, Republic of	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.165	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
203.113.9.143	Thailand	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.165	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
62.193.237.19	France	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.165	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
194.63.141.166	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
188.95.158.198	Ukraine	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.165	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
109.199.121.140	Romania	147.237.76.44	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.165	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
109.199.121.140	Romania	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.165	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
106.39.95.194	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
104.192.0.20		147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
213.210.205.2	Saudi Arabia	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.165	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
203.113.9.143	Thailand	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
188.95.158.198	Ukraine	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.165	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
188.95.158.198	Ukraine	147.237.76.42	refuah.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.165	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
109.199.121.140	Romania	147.237.76.34	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.165	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1

05-04-2015-06:03:04 to 05-04-2015-07:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.87.117.34	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	248
96.246.226.224	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
202.86.209.59	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
104.131.228.99		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
149.78.90.228	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	23
149.78.90.228	Israel	147.237.77.234	halag.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	20
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
67.78.97.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
46.19.85.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
187.233.203.194	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
68.4.81.4	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
5.102.254.70	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
77.127.230.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
76.119.70.75	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
87.68.81.229	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
207.246.197.57	United States	147.237.0.35	akaws.idf.il		drop	drop	5
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
75.70.21.209	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
81.218.59.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.93.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.102.254.70	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	4
149.129.160.231	United States	147.237.8.50	e.tikshuv.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	4
188.165.15.195	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.5	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
76.126.215.200	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
209.129.49.221	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
107.220.144.133	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.121.252.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
199.59.148.210	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
76.95.98.217	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.65.82.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.169.88	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.93.164	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.64.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.169.88	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.93.242	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.169.88	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
73.40.199.32	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.58.74.247	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	86
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	81
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	61
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	7
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	7
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	5
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	5
157.55.39.107	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
2.54.188.90	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	4
46.229.164.99	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.229.164.99	Block	3
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	3
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	2
77.66.121.242	Denmark	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
46.229.164.102	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//giyus/kadatz	Block	2
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	2
46.229.164.113	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//giyus/kadatz	Block	2
46.116.124.51	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.245	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
109.253.142.67	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.59	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
46.229.164.99	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/qanda	Block	1
66.249.93.242	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/101003-1g.stm	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Unknown Parameter 55bffe68 in www.aka.idf.il/main/home/default.aspx	None	1
46.229.164.114	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.229.164.114	Block	1
195.110.35.13	France	147.237.77.216	dover.idf.il	WordPress SoakSoak Malware - 1	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	1
66.249.64.253	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8573-he/navy.aspx	Block	1
113.178.13.220	Vietnam	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/14-en/patzar.aspx	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
2.52.179.183	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.58.74.247	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
79.181.212.254	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
46.229.164.114	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
31.193.51.59	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.78	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/giyus/general.aspx	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/military-police/	Block	1
66.249.67.51	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/994-7806-he/nakhal.aspx	Block	1
149.78.90.228	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1486-he/atal.aspx	Block	1
69.30.240.46	United States	147.237.77.234	halag.idf.il	Illegal HTTP Version	Block	1
2.54.175.187	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
180.76.4.69	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
84.228.68.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1