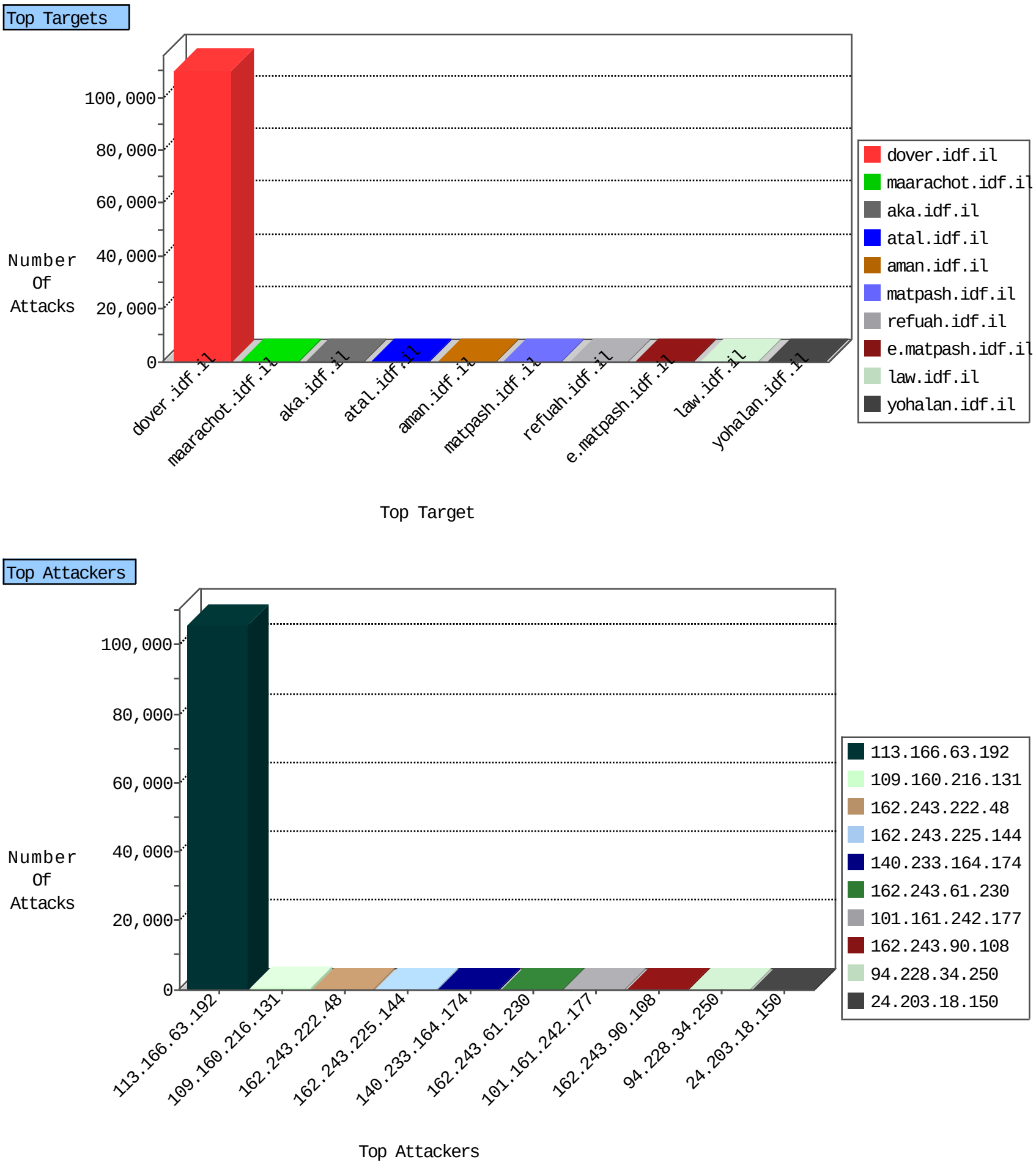
04-21-2015-05:03:04 to 04-21-2015-06:03:04

IDF Under Attack
04-21-2015-05:03:04



04-21-2015-05:03:04 to 04-21-2015-06:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	233
166.137.252.123	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	56
204.42.253.130	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
192.3.202.234	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.50	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

04-21-2015-05:03:04 to 04-21-2015-06:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	6
46.116.211.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
107.188.24.113		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	2
46.121.113.242	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
93.115.83.16	Anonymous Proxy	147.237.0.17	m.my-kosher-kravi.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
198.20.70.114	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
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	147.237.77.170	maarachot.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
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
79.178.132.78	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.20.70.114	United States	147.237.76.42	refuah.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
71.6.165.200	United States	147.237.77.178	e.matpash.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
85.25.43.94	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1

04-21-2015-05:03:04 to 04-21-2015-06:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.67.39	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	34
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.14	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.26	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
213.210.205.2	Saudi Arabia	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
199.255.137.52	United States	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
199.255.137.52	United States	147.237.77.235	sviva.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
162.253.66.6	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
5.97.89.205	Italy	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
5.97.89.205	Italy	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.66	China	147.237.77.234	halag.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
213.210.205.2	Saudi Arabia	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
199.255.137.52	United States	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.65	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
99.235.185.98	Canada	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.160.224.128	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
5.97.89.205	Italy	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1

04-21-2015-05:03:04 to 04-21-2015-06:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
113.166.63.192	Vietnam	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	105891
109.160.216.131	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	840
162.243.222.48	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	214
162.243.225.144	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	165
140.233.164.174	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	154
162.243.61.230	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	152
101.161.242.177	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	143
162.243.90.108	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	142
94.228.34.250	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	132
24.203.18.150	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	129
162.243.210.161	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	126
107.170.181.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	126
104.131.228.99		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	121
192.241.245.200	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	117
98.119.130.25	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	83
70.198.68.74	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	71
166.137.252.123	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	65
71.129.33.96	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	63
96.56.12.230	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
104.162.241.87		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
109.253.135.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
199.96.50.150	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
140.139.231.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
85.72.40.4	Greece	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
189.253.3.211	Mexico	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
109.253.140.59	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
46.120.169.142	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
84.108.220.11	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
79.178.132.78	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
37.26.147.182	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
93.173.228.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
98.15.168.87	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
79.177.37.215	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
85.64.28.184	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
207.46.13.35	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
66.249.79.74	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
31.116.149.50	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
66.29.191.97	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
88.198.157.212	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
82.80.133.244	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
71.107.27.96	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
115.64.200.148	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
207.46.13.52	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
109.253.146.211	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
177.183.248.110	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
66.249.79.58	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16

04-21-2015-05:03:04 to 04-21-2015-06:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	10
46.119.113.155	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
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
66.249.65.161	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-9070-he/atal.aspx	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/response.stm	Block	1
69.6.106.246	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 69.6.106.246	Block	1
37.142.93.248	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/iturim/iturim.aspx	None	1
157.55.39.251	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
207.46.13.35	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/hativa7/wars.stm	Block	1
69.6.106.246	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
184.105.139.68	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
207.46.13.65	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/pdf/files/5/112435.pdf).	Block	1
66.249.64.20	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI in www.aka.idf.il/main/giyus/general.aspx	None	1
188.165.15.27	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/october/9.stm	Block	1
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	1
77.237.138.202	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	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
192.34.109.234	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.156	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/894-he/idfg.aspx	Block	1

04-21-2015-05:03:04 to 04-21-2015-06:03:04