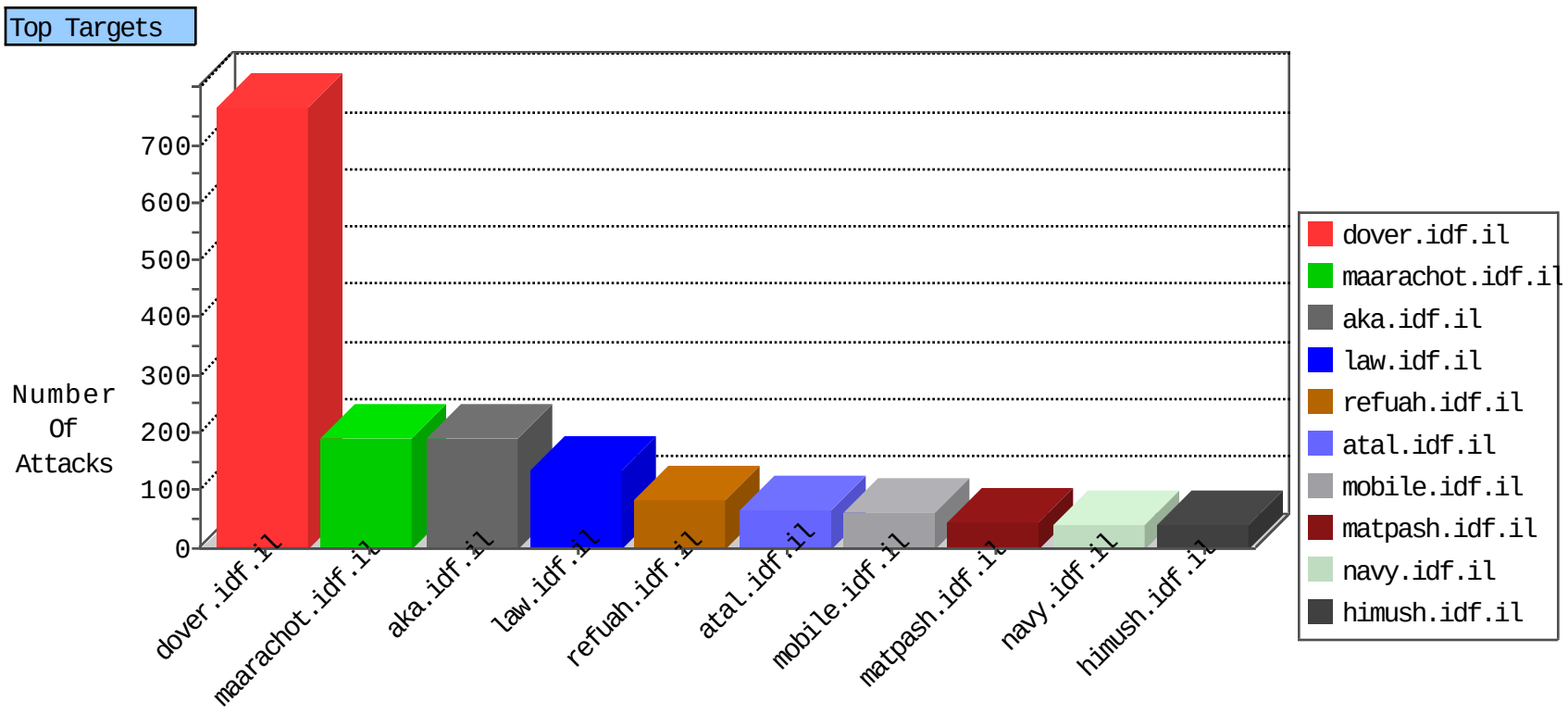
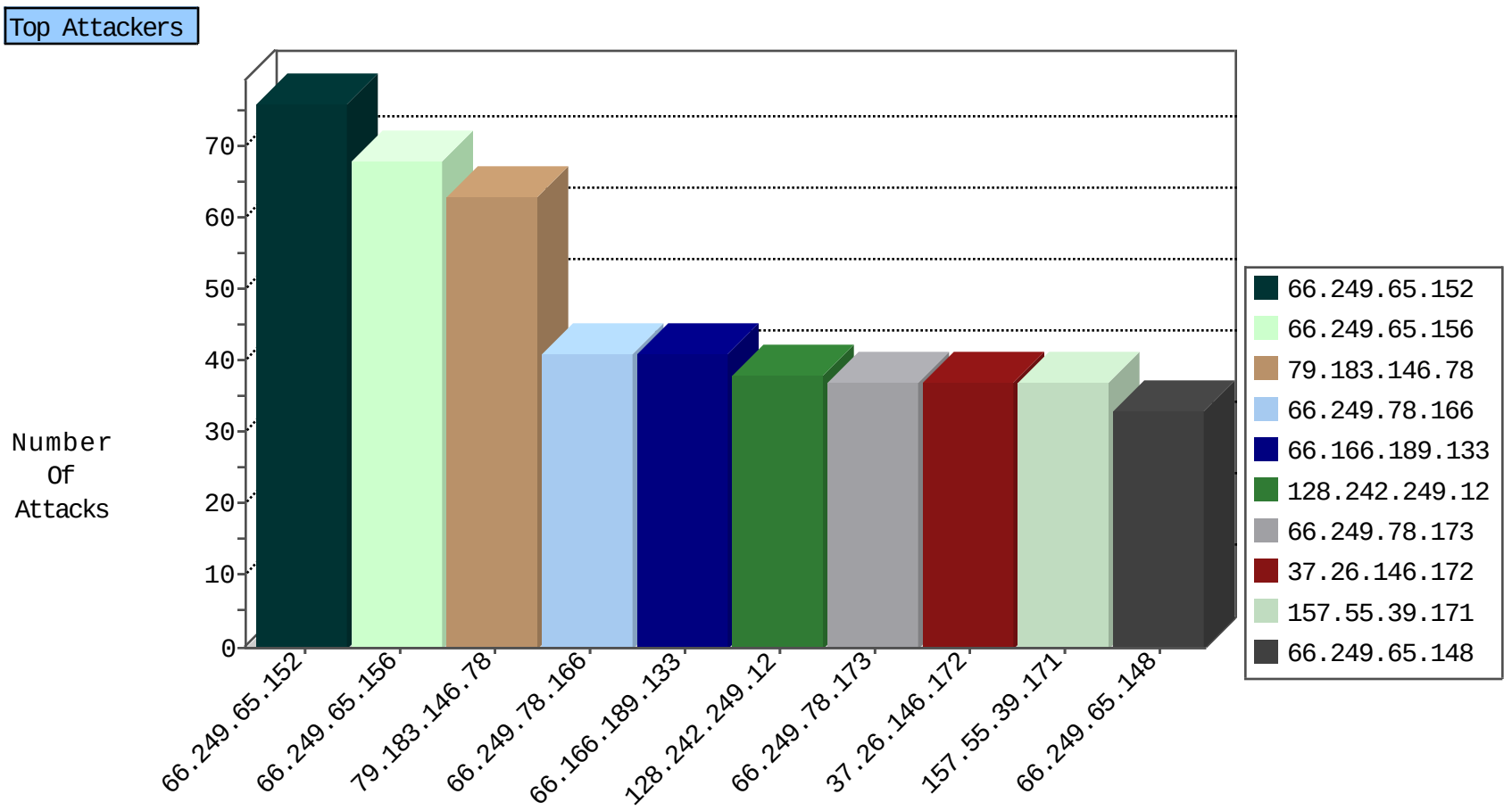
04-14-2015-01:03:04 to 04-14-2015-02:03:04

IDF Under Attack
04-14-2015-01:03:04

Top Targets



Top Attackers



04-14-2015-01:03:04 to 04-14-2015-02:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	76
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	68
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	40
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	37
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	33
66.249.73.217	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	30
66.249.65.28	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	29
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	27
66.249.73.211	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	22
66.249.73.203	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	21
66.249.65.41	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	21
66.249.65.30	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	20
66.249.73.219	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	19
66.249.73.201	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	19
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	18
66.249.65.43	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	18
66.249.65.39	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	18
66.249.65.26	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	16
66.249.65.44	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	16
66.249.65.46	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	15
66.249.65.36	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	15
66.249.93.172	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	15
66.249.65.5	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	15
66.249.65.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	15
66.249.65.3	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	14
66.249.65.32	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	14
66.249.65.195	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	13
66.249.65.181	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	13
66.249.65.52	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.67.99	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	11
66.249.65.191	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	11
66.249.65.1	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	11
66.249.65.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	11
66.249.93.176	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.65.195	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	10
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	10
66.249.65.50	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.64.146	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.73.209	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.65.48	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.65.12	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	7
66.249.89.103	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.89.105	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.65.14	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	6
66.249.65.10	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	6
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.83.182	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.65.186	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.83.188	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.64.142	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4

04-14-2015-01:03:04 to 04-14-2015-02:03:04

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	38
46.19.85.108	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	3
198.100.144.75	Canada	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	2
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.179	e.mazi.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
198.20.69.98	United States	147.237.0.200	m4u.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	147.237.8.14	e.orchot.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
85.25.103.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.216	dover.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	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.176	test.ncore.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
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1

04-14-2015-01:03:04 to 04-14-2015-02:03:04

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
218.6.132.45	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	1
208.39.68.33	United States	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 2048	1
125.5.16.195	Philippines	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
125.5.16.195	Philippines	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
85.95.238.253	Turkey	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
218.6.132.45	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 4096	1
208.39.68.33	United States	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 3072	1
208.39.68.33	United States	147.237.72.156	aman.idf.il	ET SCAN NMAP -f -sS	1
128.199.75.236	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
125.5.16.195	Philippines	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.57.151.37	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.64	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

04-14-2015-01:03:04 to 04-14-2015-02:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
79.183.146.78	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	63
66.166.189.133	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
37.26.146.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
157.55.39.171	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
209.6.236.151	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
80.246.133.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
176.12.138.101	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
62.24.222.131	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
176.12.140.166	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
176.228.130.25	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
209.129.64.2	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
176.12.145.123	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
85.250.171.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.19.85.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
109.253.135.124	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
85.250.135.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
157.55.39.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	9
213.57.133.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
62.24.222.132	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
79.182.0.151	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
176.12.137.117	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
176.12.148.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
213.172.183.61	Poland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
207.46.13.82	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
36.248.165.155	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
80.230.70.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
176.12.149.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
176.12.149.170	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.144.144	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.175	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
188.120.148.245	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	monitor	5
199.254.238.252	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.41	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.241.237.223	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
2.54.27.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.26.148.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
80.246.133.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
108.48.207.110	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4

04-14-2015-01:03:04 to 04-14-2015-02:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
91.207.7.45	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	2
199.254.238.252	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/homepage.asp	Block	2
37.59.43.170	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.6	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	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
2.54.58.222	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.210.114.129	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/8/3198.pdf/trackback/	Block	1
157.55.39.171	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.133.238	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
112.111.172.185	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/3/3593.pdf/trackback/	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
84.229.197.86	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
207.46.13.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/gaash/units.stm	Block	1
87.68.53.121	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
37.59.43.170	France	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/rights/asp/info.asp	None	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/021104-2.stm	Block	1
79.180.193.111	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
89.138.202.223	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
54.149.90.228	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/erkot.stm	Block	1
80.246.133.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1

04-14-2015-01:03:04 to 04-14-2015-02:03:04