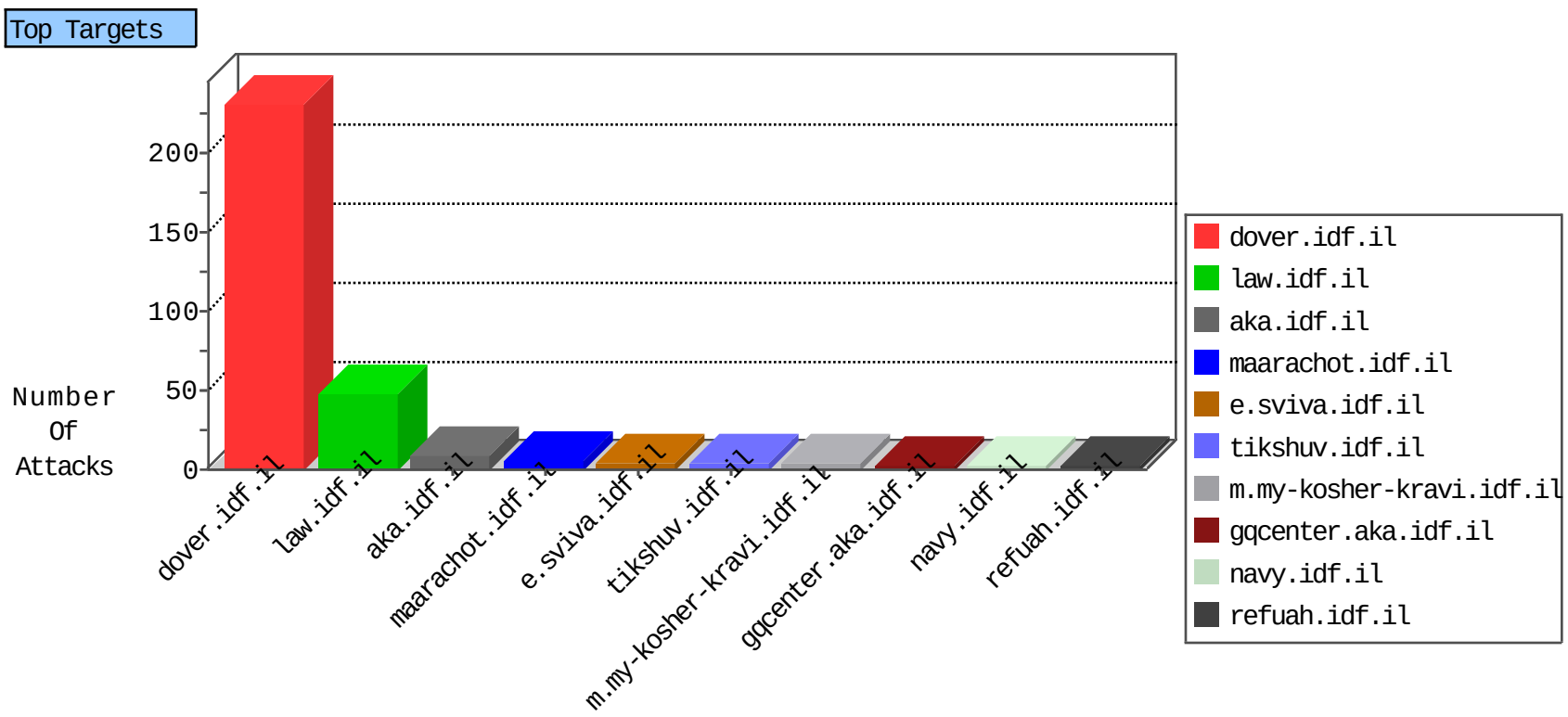
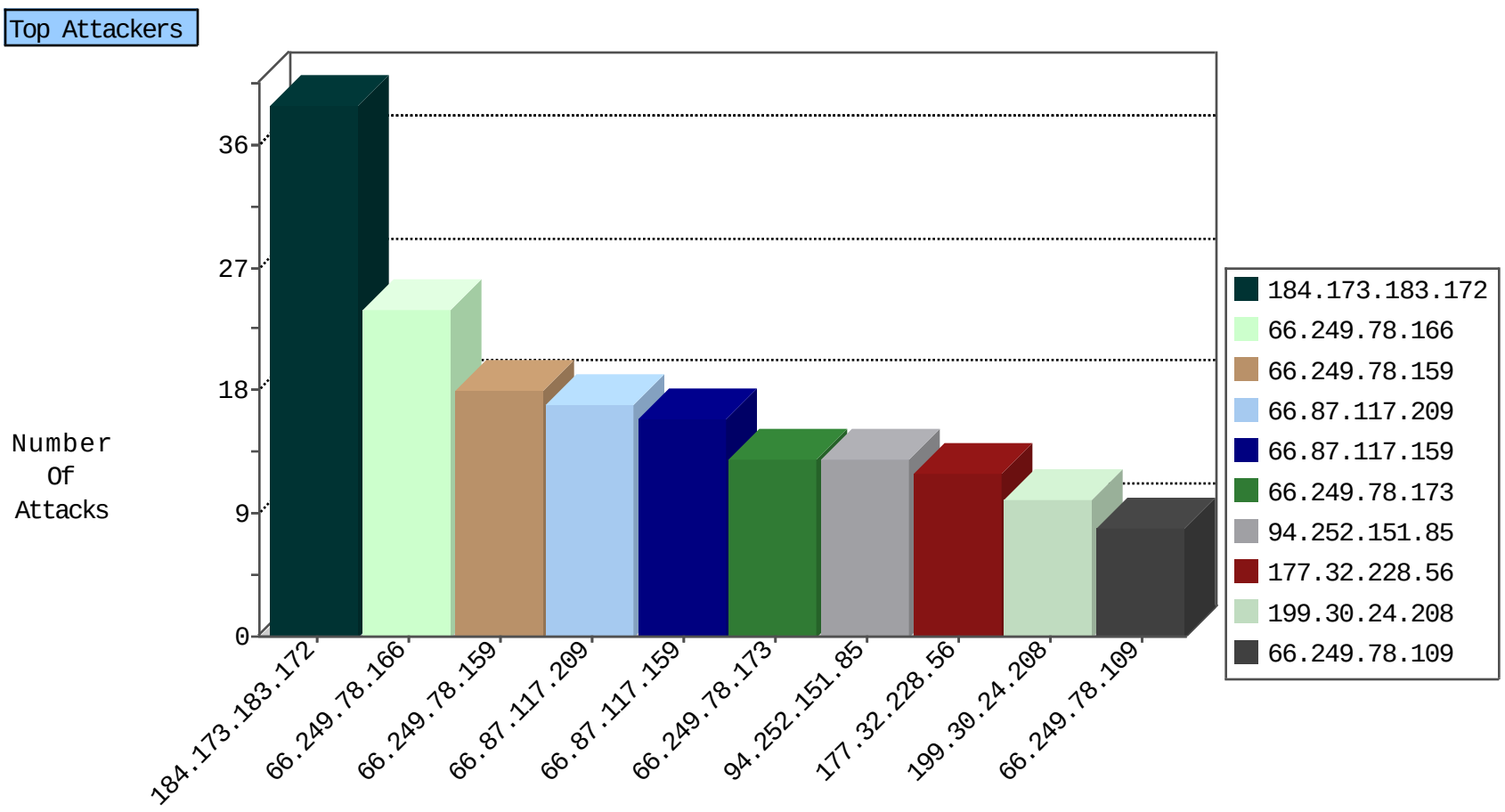
04-29-2015-03:03:04 to 04-29-2015-04:03:04

IDF Under Attack
04-29-2015-03:03:04





04-29-2015-03:03:04 to 04-29-2015-04:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.122	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	3998
66.249.67.108	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3780
66.249.67.116	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	142
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	99
220.181.108.86	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	67
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
89.163.0.214	Russian Federation	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
99.172.53.182	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
186.247.155.85	Brazil	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

04-29-2015-03:03:04 to 04-29-2015-04:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	39
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.76.147	chinuch.aka.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	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.16	my-kosher-kravi.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
85.25.103.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.170	maarachot.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
46.116.211.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-29-2015-03:03:04 to 04-29-2015-04:03:04

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
66.249.67.108	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.67	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
95.173.171.236	Turkey	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.37	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
61.240.144.67	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
104.167.117.197		147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
91.224.132.118	Russian Federation	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1

04-29-2015-03:03:04 to 04-29-2015-04:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
66.87.117.209	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
66.87.117.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
177.32.228.56	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
199.30.24.208	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
94.252.151.85	Syrian Arab Republic	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	9
203.127.58.228	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
174.95.103.193	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
220.255.1.115	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
94.252.151.85	Syrian Arab Republic	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
157.55.39.176	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
96.224.5.142	United States	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	4
186.27.163.59	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
208.54.40.134	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.78.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.190.155.182	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
68.112.56.155	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
89.178.62.86	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
1.120.166.122	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.78.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
125.209.235.177	Korea, Republic of	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
66.249.78.109	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.13	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
41.130.70.50	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
103.6.151.209	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
77.125.119.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unexpected post SYN packet - RST or SYN expected	drop	drop	1
174.236.82.233	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
1.120.166.122	Australia	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
89.178.62.86	Russian Federation	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
187.7.217.78	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.86.152	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
84.228.145.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
1.120.166.122	Australia	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
216.218.206.112	United States	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
188.138.17.205	France	147.237.76.148	gqcenter.aka.idf.i		drop	drop	1
88.198.22.112	Germany	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
203.127.96.218	Singapore	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
66.249.64.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
184.105.139.120	United States	147.237.77.227	e.hamaz.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
1.120.166.122	Australia	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
73.178.227.199	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
188.138.17.205	France	147.237.76.196	e.sviva.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

04-29-2015-03:03:04 to 04-29-2015-04:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-15745-en/dover.aspx	Block	1
66.249.64.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-he/dover.aspx	Block	1
96.224.5.142	United States	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.stm	Block	1
66.249.69.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
180.76.5.17	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1106-6.stm	Block	1
72.46.135.146	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16246-he/dover.aspx	Block	1
66.249.64.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
125.209.235.177	Korea, Republic of	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
66.249.69.36	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
212.199.136.107	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
74.82.47.3	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.78.120	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/m/	Block	1
66.249.64.40	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//1153-he/dover.aspx	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/home.asp/news.asp	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
66.249.75.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
88.198.22.112	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 88.198.22.112	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
66.249.64.74	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1133-en/hamaz.aspx	Block	1
157.55.39.247	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/news.aspx	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.95	Block	1
64.19.78.240	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
88.198.22.112	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ie-welcome.stm	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/catalog.asp	Block	1
66.249.67.84	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
173.48.34.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/	Block	1
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	1

04-29-2015-03:03:04 to 04-29-2015-04:03:04