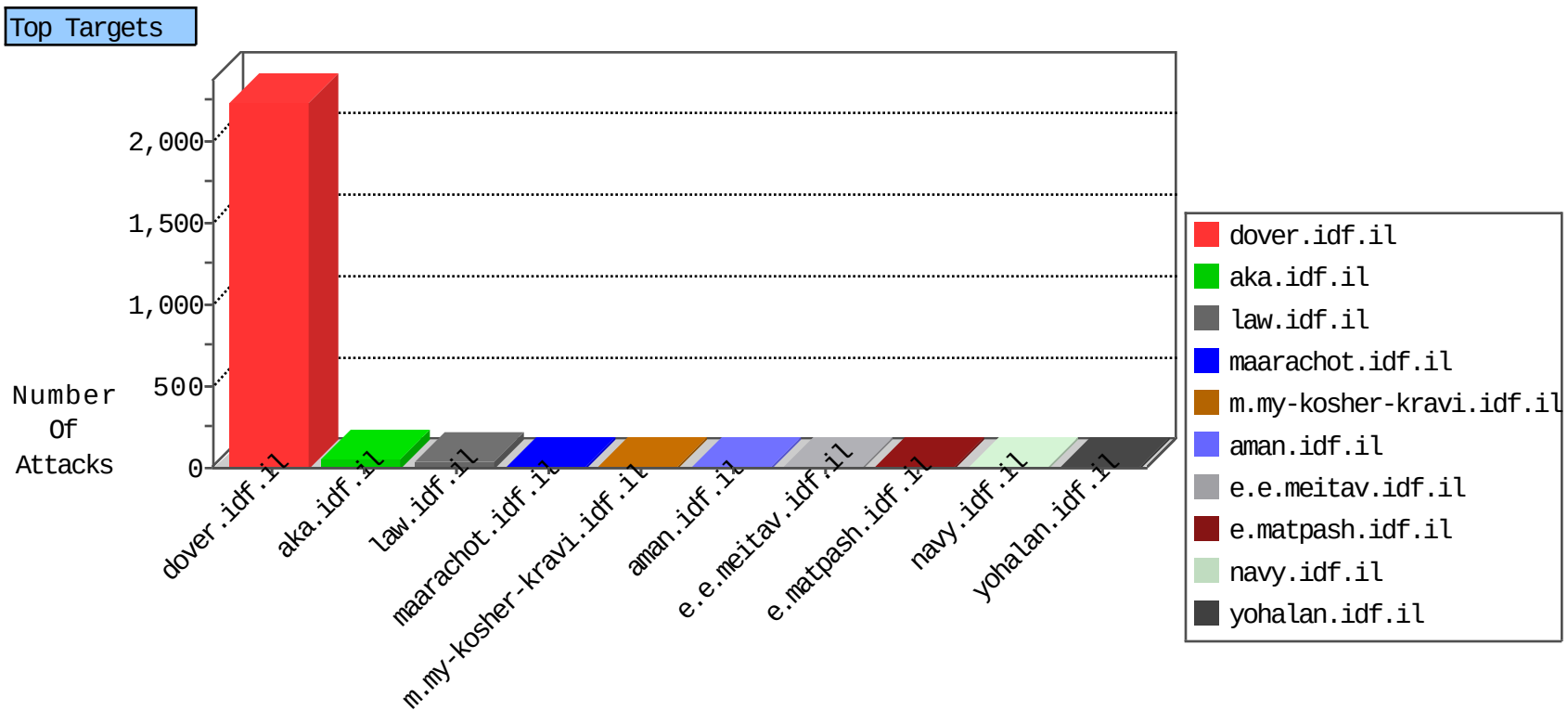
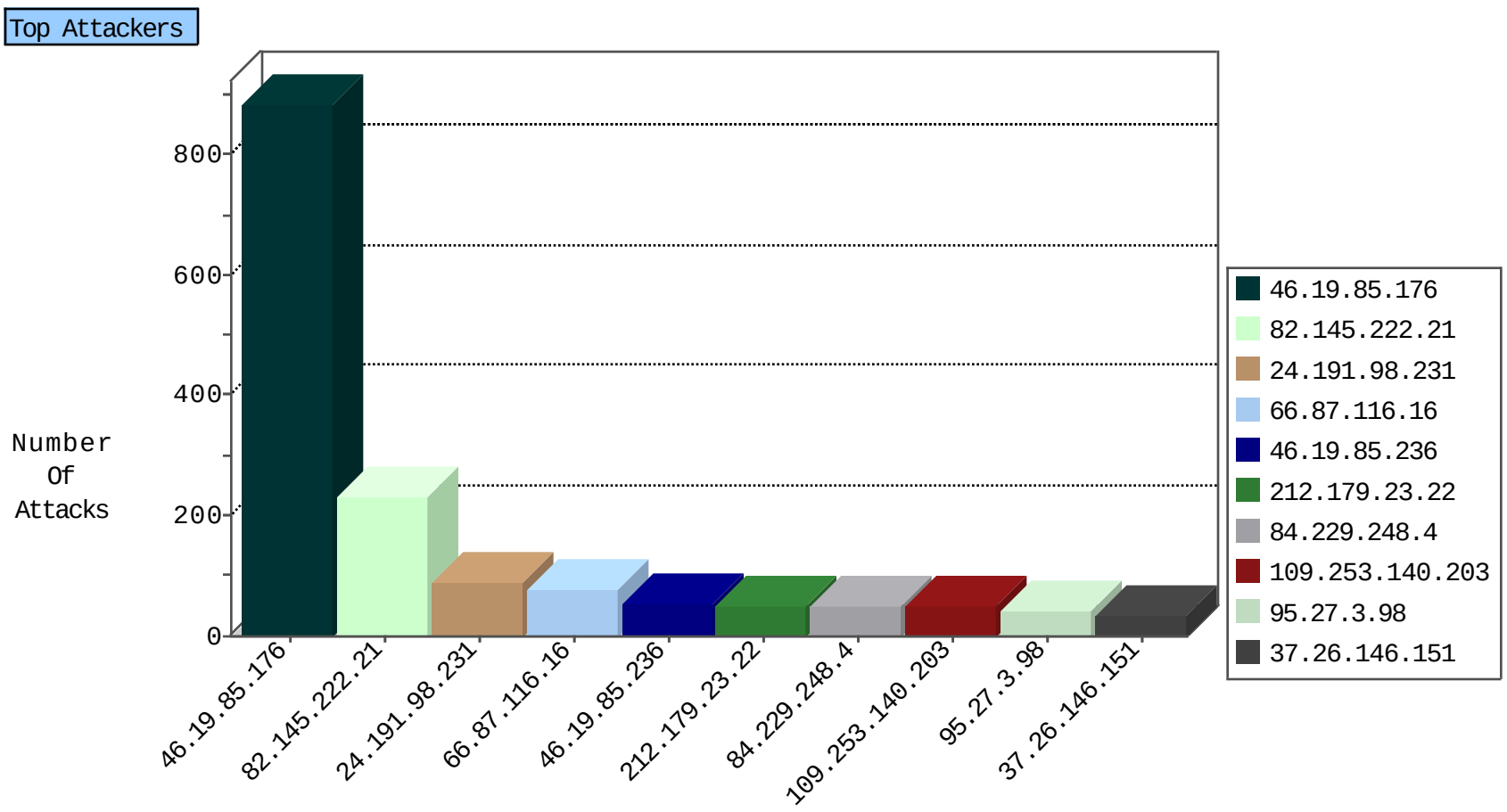
04-20-2015-06:03:03 to 04-20-2015-07:03:03

IDF Under Attack
04-20-2015-06:03:03





04-20-2015-06:03:03 to 04-20-2015-07:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3311
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	212
84.108.63.114	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	169
106.243.103.207	Korea, Republic of	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	2
188.138.9.50	Germany	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
204.8.154.50	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
204.8.154.50	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

04-20-2015-06:03:03 to 04-20-2015-07:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
36.224.164.208	Taiwan	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_P-N_40-59	Permit	3
198.20.70.114	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.250.88.65	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.198	e.yohalan.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	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.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
85.25.103.50	Germany	147.237.0.15	kosher-kravi.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
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1

04-20-2015-06:03:03 to 04-20-2015-07:03:03

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
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
58.132.169.187	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
58.132.169.187	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
104.245.99.48		147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.132.169.187	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
58.132.169.187	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
58.132.169.187	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
209.239.114.179	United States	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
91.217.90.49	Ukraine	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.14	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.240.144.67	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.132.169.187	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1

04-20-2015-06:03:03 to 04-20-2015-07:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.85.176	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	886
82.145.222.21	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	231
24.191.98.231	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	89
66.87.116.16	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	77
46.19.85.236	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
212.179.23.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
84.229.248.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
109.253.140.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
95.27.3.98	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
37.26.146.151	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
2.52.36.15	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
68.150.109.224	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
50.88.138.208	United States	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	30
213.57.225.7	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
82.166.191.249	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
176.12.138.204	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
2.52.181.40	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
93.172.81.81	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
84.228.172.162	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
190.92.27.116	Honduras	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
157.55.39.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
176.12.144.18	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
91.135.102.184	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
24.44.104.30	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
207.46.13.52	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
77.127.71.75	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
204.237.22.235	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
168.63.200.167	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
207.46.13.35	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
46.19.85.112	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
109.253.136.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
174.99.27.143	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
66.249.64.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
99.234.146.147	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
46.19.85.78	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
198.200.65.67	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
193.169.234.5	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
194.90.99.193	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
1.136.96.119	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6

04-20-2015-06:03:03 to 04-20-2015-07:03:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.70.80	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	2
176.12.138.204	Israel	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
84.228.111.51	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
184.105.139.68	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
66.249.64.14	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
104.162.147.46		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.73.221	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
46.19.85.171	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
188.165.15.27	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.64.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20420-he/dover.aspx	Block	1
46.19.85.195	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.223	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/â€Ž	Block	1
70.167.8.42	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/870-he/sb_item_lev2	Block	1
66.249.67.143	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20095-he/idfgdover.aspx	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
216.218.206.68	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
5.28.167.184	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
176.12.144.18	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19646-he/dover.aspx	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
31.193.51.84	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1

04-20-2015-06:03:03 to 04-20-2015-07:03:03