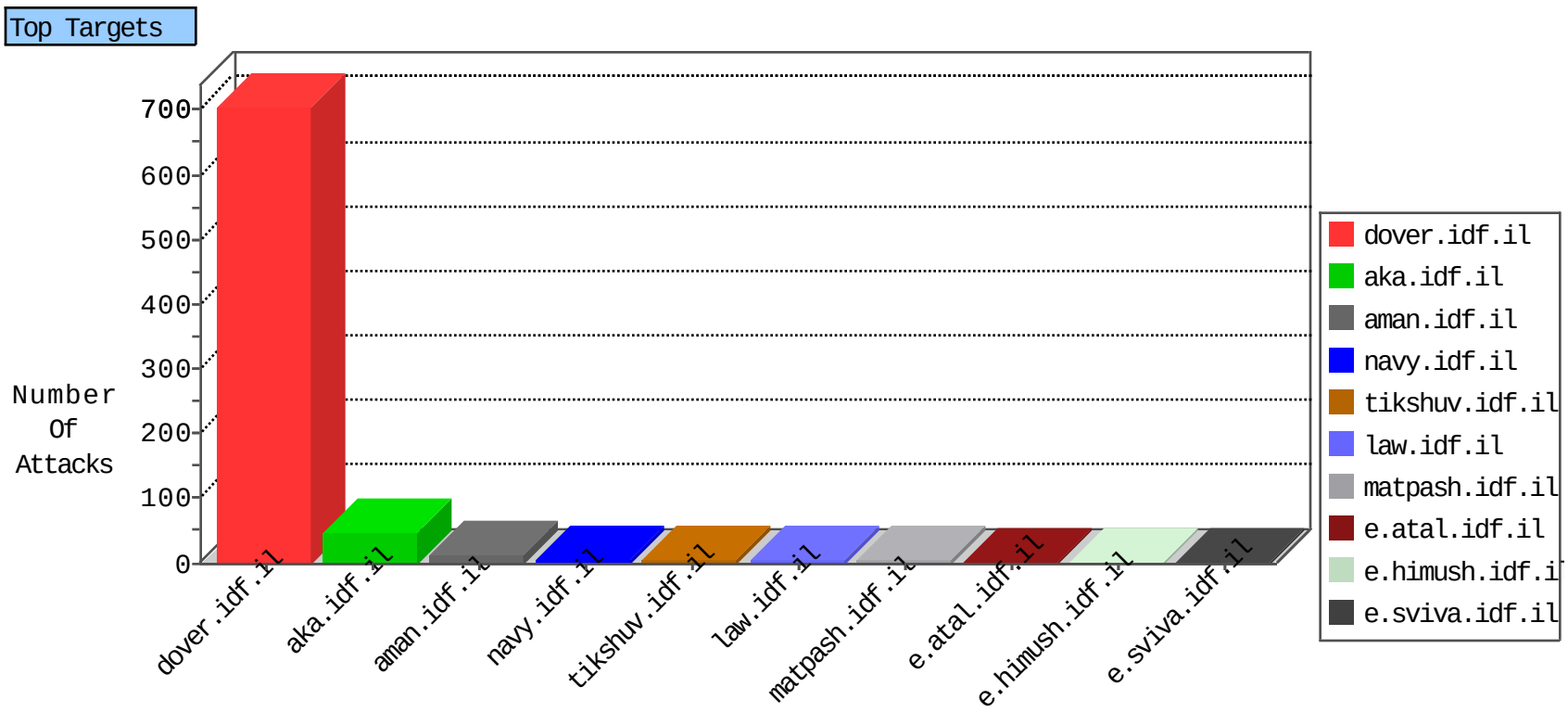
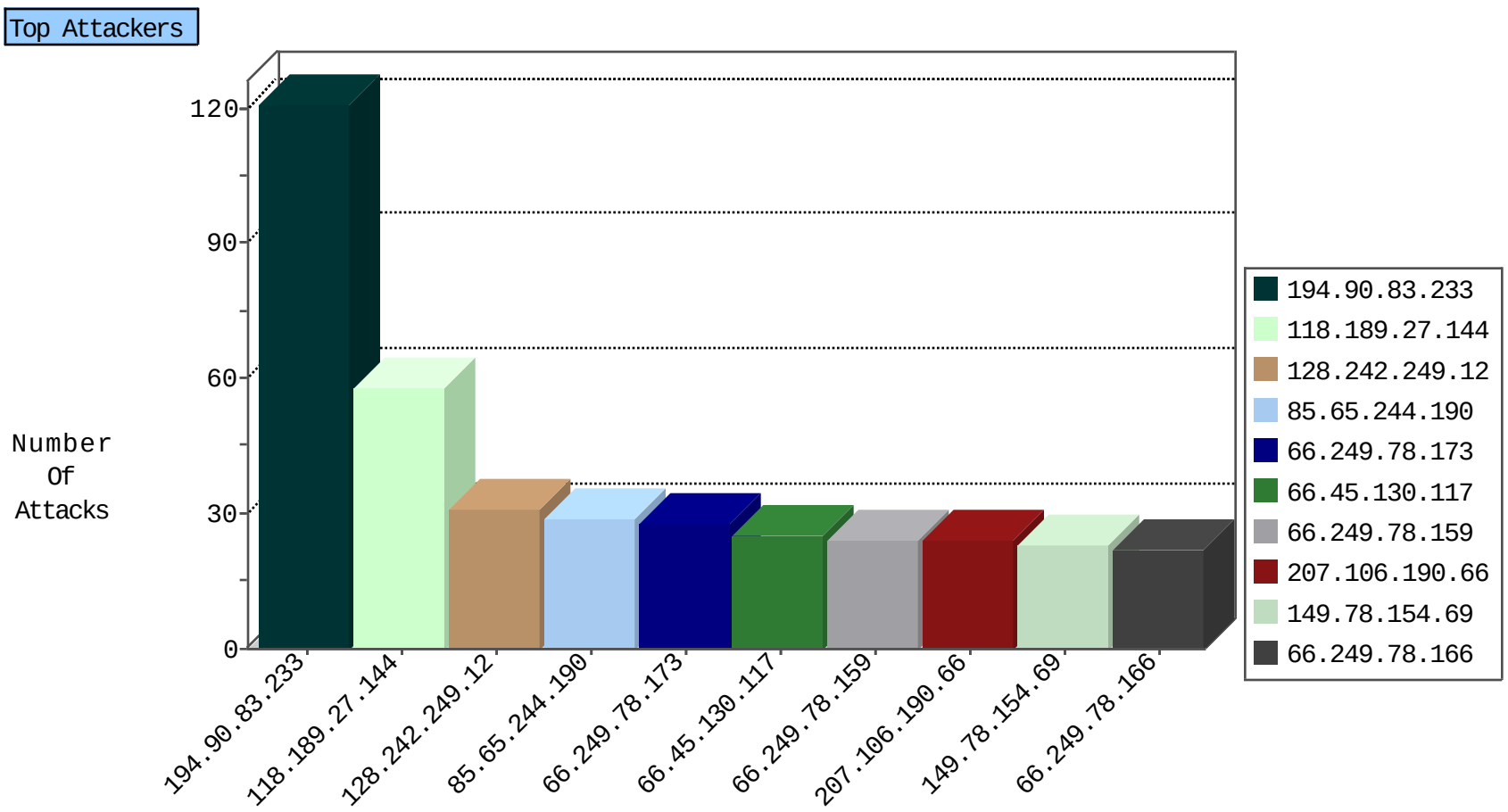
05-06-2015-06:03:02 to 05-06-2015-07:03:02

IDF Under Attack
05-06-2015-06:03:02

Top Targets



Top Attackers



05-06-2015-06:03:02 to 05-06-2015-07:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	339
80.246.138.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
66.249.73.209	Israel	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	3
138.134.102.15	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
124.232.142.220	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
220.255.1.175	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
146.185.239.100	Russian Federation	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

05-06-2015-06:03:02 to 05-06-2015-07:03:02

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	29
112.111.189.8	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	3
36.231.145.10	Taiwan	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	3
106.68.68.145	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.77.74	law.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	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.205	prisha.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
46.121.246.188	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1

05-06-2015-06:03:02 to 05-06-2015-07:03:02

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	7
109.65.142.119	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
188.138.9.51	Germany	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.165.220.215	Germany	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
188.138.9.51	Germany	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
46.165.220.215	Germany	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
46.165.220.215	Germany	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

05-06-2015-06:03:02 to 05-06-2015-07:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
194.90.83.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	118
118.189.27.144	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
85.65.244.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
66.45.130.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.66.21.27	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
37.26.148.240	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
32.215.162.246	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
2.54.5.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
112.210.124.115	Philippines	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
109.64.26.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.23.113.14	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
220.255.1.153	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
220.255.1.155	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
79.178.139.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
79.179.60.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
94.230.86.226	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
37.60.147.29	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
94.230.86.226	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
111.206.36.18	China	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.136.232	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
94.230.86.240	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
171.98.76.157	Thailand	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
208.69.40.107	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
176.12.136.232	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
94.230.86.240	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
85.64.167.43	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
94.159.223.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
173.252.73.115	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
62.219.245.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
205.203.135.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
71.76.242.94	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
80.74.110.141	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
220.255.1.133	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
212.235.89.237	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
54.224.21.23	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
112.74.87.10	China	147.237.77.61	e.cogat.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	2
77.126.90.151	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

05-06-2015-06:03:02 to 05-06-2015-07:03:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
207.106.190.66	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	13
207.106.190.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.106.190.66	Block	11
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
93.172.167.148	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//newsite/english/main.stm	Block	2
207.46.13.3	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//captcha.ashx	Block	2
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.99	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/links.aspx	Block	1
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1540-13036-he/dover.aspx target=	Block	1
180.76.4.250	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
66.249.73.238	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//modiin/general	Block	1
195.154.181.152	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/manager/	Block	1
2.52.59.82	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.124	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/0828-3.stm	Block	1
66.249.65.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
184.105.247.195	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
95.86.111.32	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	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
195.154.216.165	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/101003-1g.stm	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
82.166.72.200	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.65.188	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
185.61.138.244		147.237.77.176	matpash.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.66.107.90	Israel	147.237.77.74	law.idf.il	Redundant HTTP Headers Referer	Block	1
27.74.214.91	Vietnam	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.204	Block	1
85.65.210.40	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.73.230	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//modiin/general	Block	1
213.157.46.31	Kazakstan	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
188.165.15.240	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
125.27.173.94	Thailand	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/	Block	1
49.230.83.11	Thailand	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13104-en/dover.aspx forcerecrawl: 0	Block	1
85.250.138.71	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.73.230	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/general	Block	1
195.154.181.152	France	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 195.154.181.152	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

05-06-2015-06:03:02 to 05-06-2015-07:03:02