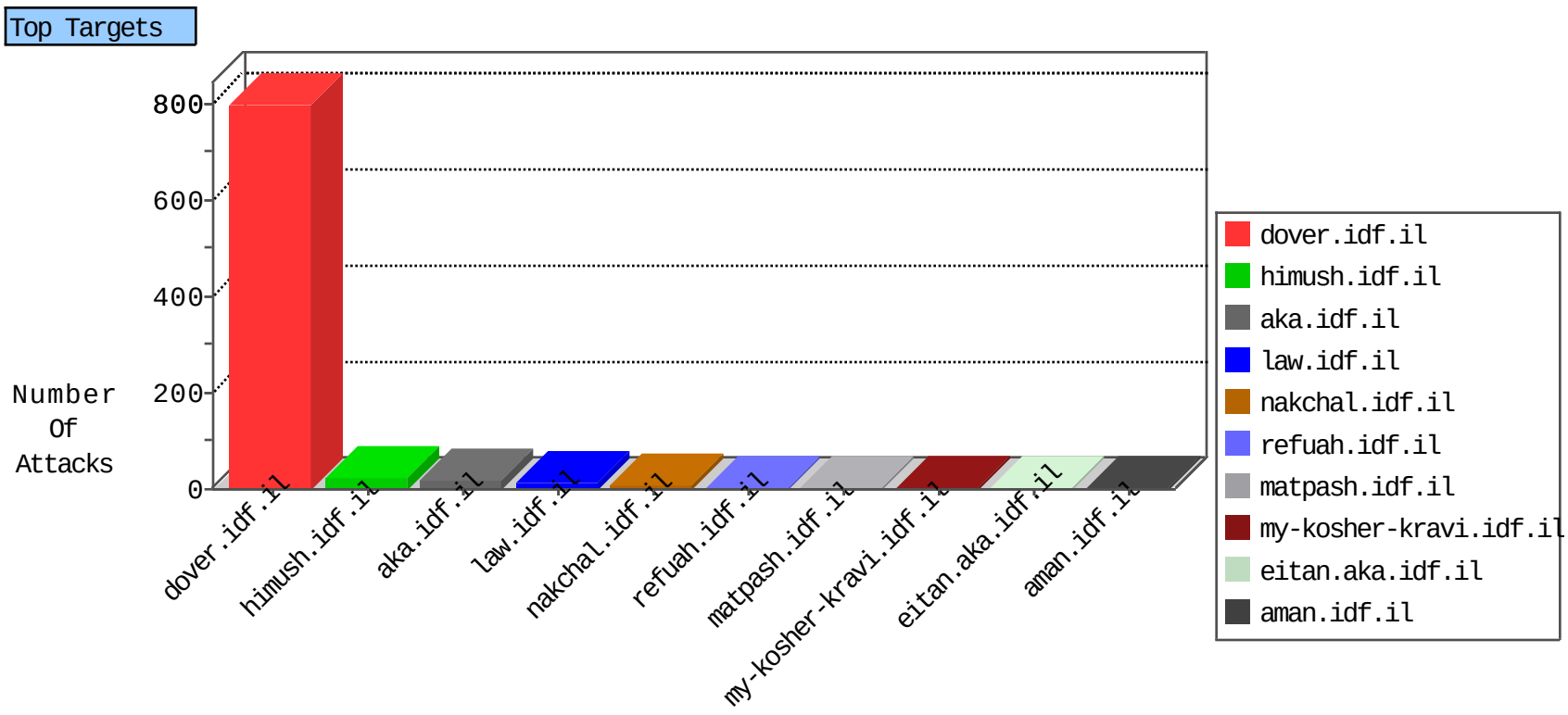
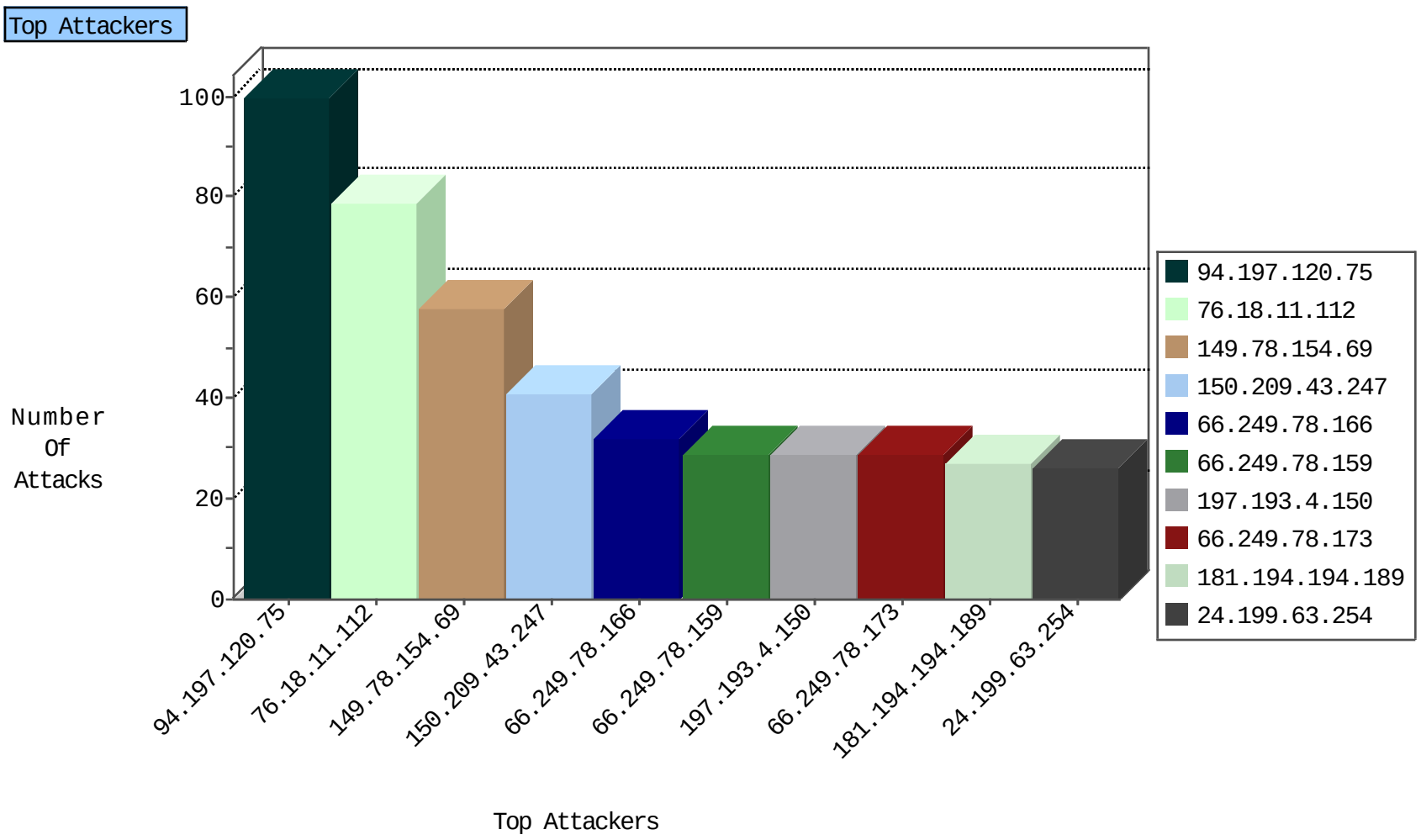
05-06-2015-03:03:00 to 05-06-2015-04:03:00

IDF Under Attack
05-06-2015-03:03:00





05-06-2015-03:03:00 to 05-06-2015-04:03:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.88	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	95
66.249.64.148	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	60
82.145.211.12	Europe	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	8
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
104.255.66.201		147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
104.255.66.201		147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
104.255.66.201		147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

05-06-2015-03:03:00 to 05-06-2015-04:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
198.20.69.98	United States	147.237.76.176	test.ncore.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
122.2.21.141	Philippines	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
71.6.135.131	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.142	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.235	sviva.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

05-06-2015-03:03:00 to 05-06-2015-04:03:00

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
109.253.157.64	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
66.249.64.148	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	1
188.138.9.51	Germany	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.75.56.43		147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
164.138.239.226	Iraq	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
162.248.166.125	Canada	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
110.93.224.68	Pakistan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
110.93.224.68	Pakistan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
213.210.205.2	Saudi Arabia	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.75.56.43		147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
162.248.166.125	Canada	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
110.93.224.68	Pakistan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
110.93.224.68	Pakistan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
213.210.205.2	Saudi Arabia	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
110.93.224.68	Pakistan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
213.210.205.2	Saudi Arabia	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1

05-06-2015-03:03:00 to 05-06-2015-04:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
94.197.120.75	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	100
76.18.11.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	79
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
150.209.43.247	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
197.193.4.150	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
181.194.194.189	Costa Rica	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
66.176.109.184	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
24.199.63.254	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
66.249.83.182	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
104.240.107.52		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
149.144.151.102	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
118.241.234.224	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
109.253.157.64	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	monitor	11
220.255.1.172	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
24.199.63.254	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.83.194	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
157.55.39.136	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.253.157.64	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
201.120.118.231	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
104.35.90.139		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
23.117.12.126	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
188.165.15.99	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
142.179.248.139	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
41.250.141.216	Morocco	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.26.146.175	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
77.126.90.151	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
70.39.157.197	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
66.249.83.188	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
86.108.73.132	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
70.39.157.199	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
73.31.99.161	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
82.22.206.225	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
220.181.108.173	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
68.196.58.107	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
24.21.194.243	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.12.139.207	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

05-06-2015-03:03:00 to 05-06-2015-04:03:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
217.12.204.155	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	6
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	3
77.75.77.17	Czech Republic	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.75.77.17	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
52.6.169.50	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	2
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
106.6.191.125	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.64.156	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
157.55.39.81	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
180.76.5.74	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/ramon.stm	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim.	Block	1
66.249.65.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/haredim/general.aspx	Block	1
74.82.47.2	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
188.165.15.99	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.99	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/kiosk/	Block	1
157.55.39.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13169-en/dover.aspx forcerecrawl: 0	Block	1
54.145.209.107	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/â€Ž	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.67	Block	1
66.249.67.218	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1536-he/refuah.aspx	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13091-en/dover.aspx forcerecrawl: 0	Block	1
77.75.77.17	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
54.166.33.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/coni/english/main_index.stm	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1

05-06-2015-03:03:00 to 05-06-2015-04:03:00