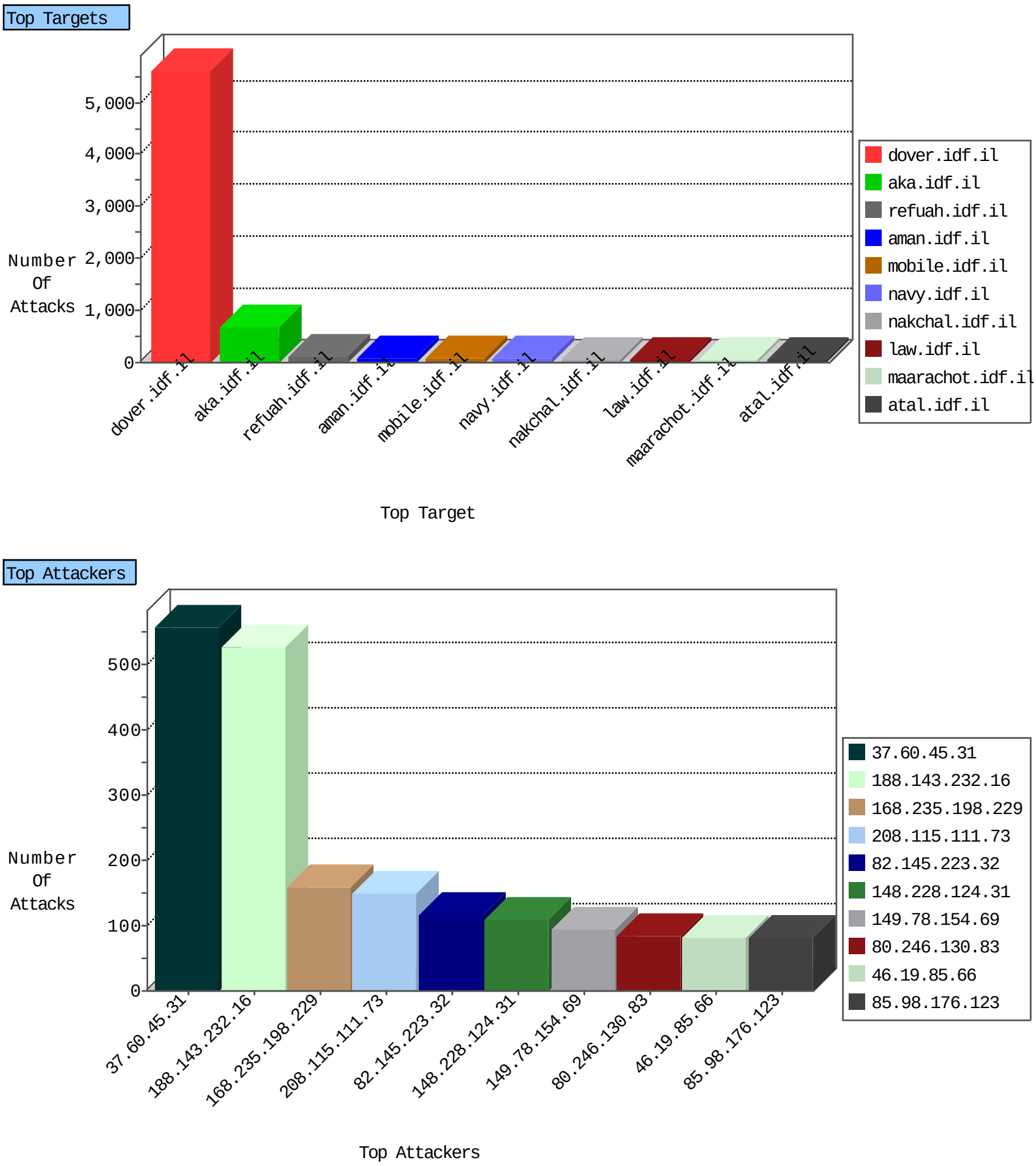
10-19-2015-19:04:06 to 10-19-2015-20:04:06

IDF Under Attack Daily Report



10-19-2015-19:04:06 to 10-19-2015-20:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	49
5.102.254.172	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
109.64.17.9	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
109.186.43.126	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
2.54.183.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
66.249.67.53	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
176.12.137.211	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.85.210	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
192.114.7.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.121.100.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
31.168.113.167	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
84.94.182.229	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
87.69.169.178	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
37.26.148.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
188.143.232.16	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
37.8.28.38	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
46.121.59.197	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
93.174.93.146	Netherlands	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
46.121.59.197	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
142.54.172.101	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
71.6.167.142	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
100.100.87.247		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
142.54.174.67	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	drop	1
46.19.86.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
192.168.1.104		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-19-2015-19:04:06 to 10-19-2015-20:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.64.116	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

10-19-2015-19:04:06 to 10-19-2015-20:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
181.177.245.75	147.237.77.234	Peru	halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
116.31.103.100	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
109.66.37.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.243.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.168.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.144.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.33.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.164.194.38	147.237.76.30	Taiwan	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.143.180.44	147.237.77.205	Germany	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
185.120.126.20	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
181.177.245.75	147.237.77.234	Peru	halag.idf.il	ET SCAN NMAP -sS window 2048	1
46.120.212.41	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
181.177.245.75	147.237.77.234	Peru	halag.idf.il	ET SCAN NMAP -f -sS	1
46.19.86.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.208.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.209.33.151	147.237.76.34	Germany	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.64.254.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.28.168.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.41.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.63.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
219.77.19.4	147.237.77.227	Hong Kong	e.hamaz.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.181.97.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
67.194.229.137	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.245	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
49.236.206.106	147.237.76.147	Malaysia	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1

10-19-2015-19:04:06 to 10-19-2015-20:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.60.45.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	557
188.143.232.16	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	371
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	148
82.145.223.32	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	116
168.235.198.229	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	114
148.228.124.31	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
46.19.85.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
80.246.130.83	Israel	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	69
66.87.98.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
192.114.91.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
85.64.89.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
178.138.98.123	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
149.78.40.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
166.137.139.60	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
46.121.159.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
79.179.140.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
67.141.165.226	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
41.13.8.155	South Africa	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
176.13.7.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
46.19.85.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
188.161.104.217	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
66.214.14.24	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
87.69.244.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
2.54.36.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
46.121.69.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
46.19.85.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
79.180.192.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
31.168.113.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
46.19.86.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
2.54.28.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
64.229.49.203	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
46.116.135.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
100.100.69.75		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
96.57.116.226	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
95.86.73.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
80.246.133.188	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	25
37.142.68.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.142.237.154	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	24
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24

10-19-2015-19:04:06 to 10-19-2015-20:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.143.232.16	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.16	Block	117
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	52
84.111.36.103	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.111.36.103	Block	39
105.159.149.205	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.159.149.205	Block	39
188.143.232.16	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	26
46.19.86.240	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	26
168.235.198.229	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 168.235.198.229	Block	26
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
66.249.67.247	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	13
109.65.151.42	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 109.65.151.42	Block	13
85.98.176.123	Turkey	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	13
79.176.191.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/×—×™×œ× ×″×?×•×™ ×¨/home/default.aspx	Block	13
212.34.11.65	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22600-ar/dover.aspx)	Block	13
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter utm_campaign in www.aka.idf.il/main/rabanut/general.aspx	None	13
87.68.40.34	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	13
84.108.249.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	13
192.116.169.9	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/imagevideogallerylobby/imagevideogallerylobby.js	Block	13
66.249.81.141	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/1746-he/lifestyle.aspx	Block	13
46.117.214.151	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
109.67.68.115	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/https:/aka.idf.il/	Block	13
85.98.176.123	Turkey	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	13
79.180.56.149	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	13
168.235.198.229	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shavascript	Block	13
87.69.38.156	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
199.16.156.125	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/6/size220x0/17416.jpg	Block	13
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
62.90.163.46	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	13
109.67.68.115	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
85.98.176.123	Turkey	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	13
80.246.130.83	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	13
182.118.45.215	China	147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/../shared/clientscripts/scroller/jquery.jcarousel.js	Block	13
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
84.111.36.103	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/yahash2015/sheelon.aspx	Block	13
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9032-he/refuah.aspx	Block	13
199.59.148.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/17416.jpg	Block	13
62.90.163.46	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	13
109.67.206.83	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	13
85.98.176.123	Turkey	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/	Block	13
80.246.139.232	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	13
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
2.52.62.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyus	Block	13
105.159.149.205	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar=123	Block	13
84.228.65.131	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/	Block	13
62.219.137.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	13
149.88.123.109	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	13
85.250.66.47	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
83.17.122.250	Poland	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	13

10-19-2015-19:04:06 to 10-19-2015-20:04:06