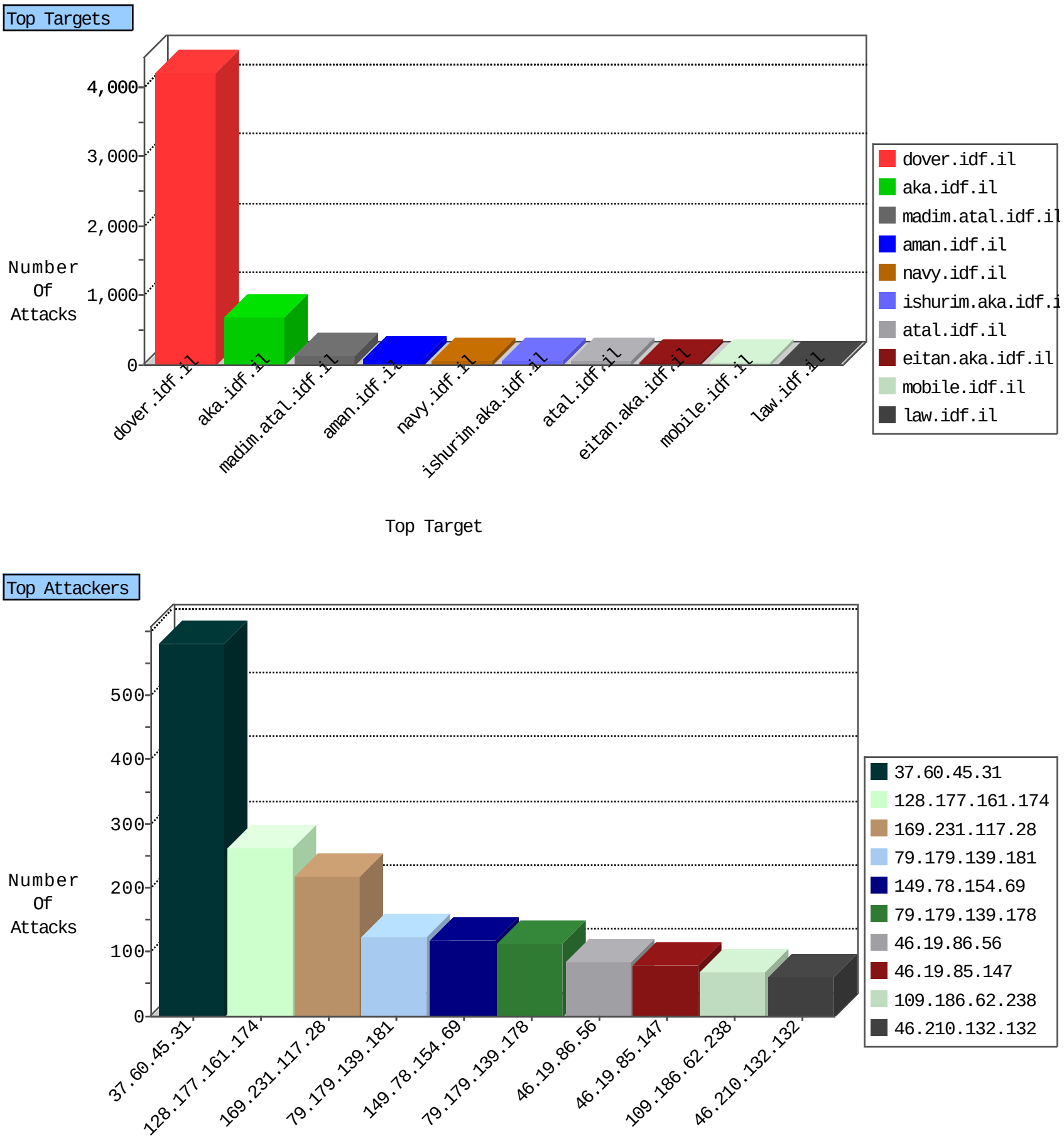
10-20-2015-23:04:07 to 10-21-2015-00:04:07

IDF Under Attack Daily Report



10-20-2015-23:04:07 to 10-21-2015-00:04:07

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	211
2.54.191.100	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	52
77.125.127.29	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
84.109.154.36	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
87.69.239.42	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	21
199.64.7.54	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
109.186.62.238	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
80.246.136.107	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
87.68.250.198	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
37.26.148.224	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
149.78.216.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
173.46.233.232	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.120.195.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.108.67.21	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
62.128.45.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.52.10.18	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	5
82.80.159.129	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
80.179.220.201	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
185.120.126.12		147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
94.230.86.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.179.139.178	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
85.64.115.192	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
84.108.64.81	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
197.200.67.56	Algeria	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.86.148	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
109.64.177.192	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.120.159.133	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
87.69.240.9	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
24.168.114.53	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
71.6.165.200	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
87.68.250.198	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
62.158.139.113	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
176.13.20.99	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
213.57.49.6	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
93.174.93.146	Netherlands	147.237.0.19	madim.atal.idf.il	Invalid TCP Flags	drop	1

10-20-2015-23:04:07 to 10-21-2015-00:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-20-2015-23:04:07 to 10-21-2015-00:04:07

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
84.228.48.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
54.236.155.16	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.7.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.41.67.92	147.237.77.74	United States	law.idf.il	ET SCAN Potential SSH Scan	1
209.41.67.92	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
159.226.230.13	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
107.150.55.78	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.105.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.7.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
52.26.42.110	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
213.14.140.166	147.237.76.31	Turkey	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
209.41.67.92	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
202.79.243.160	147.237.77.216	Japan	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.100.85.71	147.237.77.178		e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
107.150.55.78	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
89.143.162.77	147.237.72.217	Slovenia	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-20-2015-23:04:07 to 10-21-2015-00:04:07

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	582
128.177.161.174	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	263
169.231.117.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	217
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	118
79.179.139.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	99
46.19.86.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
46.210.132.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
109.186.62.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
176.13.3.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
46.19.86.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
5.29.19.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
86.46.127.45	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
163.158.101.187	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
149.78.92.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
84.108.235.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
46.19.86.58	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
100.100.9.106		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	41
93.172.157.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
198.214.249.125	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
199.64.7.54	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
77.125.127.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
100.100.53.26		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	33
71.227.74.58	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
79.177.8.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
66.102.7.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
199.189.193.5	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
79.181.2.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
79.177.31.225	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
2.54.191.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.19.86.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
5.22.129.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.86.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
46.120.159.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
164.76.64.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
213.57.49.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
2.52.10.18	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
31.154.179.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
84.109.154.36	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
87.68.250.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
2.52.63.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19

10-20-2015-23:04:07 to 10-21-2015-00:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.139.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Unauthorized URL Access on madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	104
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	52
46.19.85.147	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	52
79.180.57.135	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	39
192.99.12.99	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	26
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	26
79.179.139.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Unauthorized URL Access on madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	26
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	13
2.54.57.237	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
79.182.167.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
46.117.218.109	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	13
180.153.186.100	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery.plugins/slider.js	Block	13
79.179.112.54	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	13
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	13
5.29.196.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
80.230.17.114	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aka	Block	13
73.22.155.10	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
46.120.42.87	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	13
37.26.147.207	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	13
87.69.240.9	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 87.69.240.9	Block	13
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	13
46.120.84.225	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	13
218.54.149.67	Korea, Republic of	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/manager/html	Block	13
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	13
45.33.9.22		147.237.72.166	aka.idf.il	Oracle vulnerable procedures/functions access-January patch 117	Block	13
109.64.6.22	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
79.179.49.102	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.179.49.102 (Unknown SSL Session)	None	13
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	13
2.52.18.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
218.54.149.67	Korea, Republic of	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/manager/html	Block	13
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	13
149.88.54.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
79.179.49.102	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	13

10-20-2015-23:04:07 to 10-21-2015-00:04:07