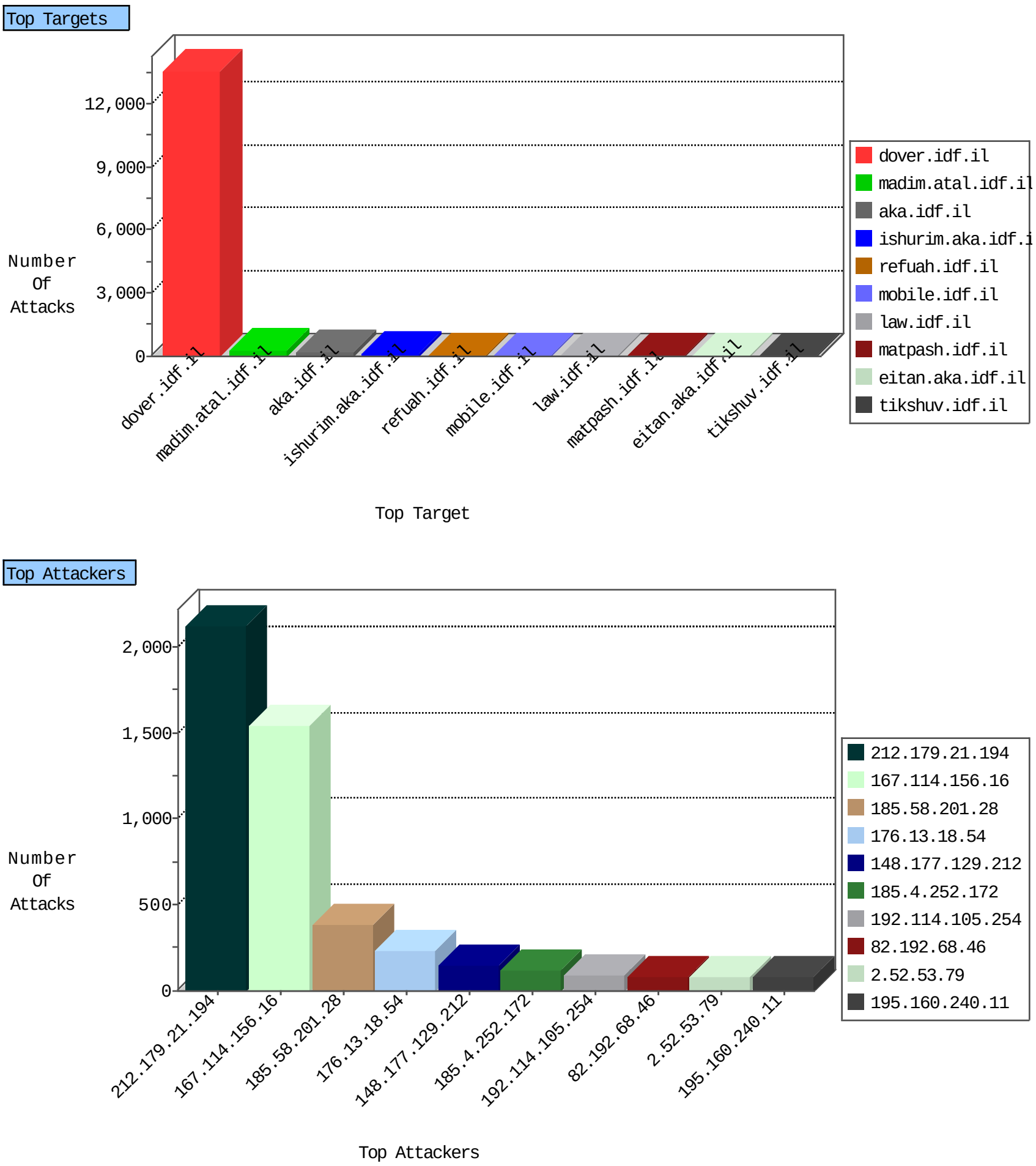
11-05-2015-09:04:07 to 11-05-2015-10:04:07

IDF Under Attack
Daily Report



11-05-2015-09:04:07 to 11-05-2015-10:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2209
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	693
66.249.79.16	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	144
66.249.79.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	129
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	42
84.108.74.76	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
2.54.62.177	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
37.26.149.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
2.54.168.121	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
2.52.53.79	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
81.218.235.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
2.54.36.148	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
87.68.83.23	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
82.80.135.174	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
80.246.137.156	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
199.203.215.1	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
176.13.6.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.52.131.12	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.179.10.173	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.18.238	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.165.173	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
31.210.189.221	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
85.250.83.79	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.179.6.127	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.108.72.137	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.52	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
185.32.179.179	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.136.35	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.160.158.184	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.47	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
87.69.184.239	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.52.51.186	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.66.133.67	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.136.200	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.51	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
185.32.179.142	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.136.19	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
77.125.109.209	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.67.124.99	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.110	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.136.232	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.18.54	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
109.65.107.162	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
148.177.129.210	Europe	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.178.25.213	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
5.144.49.160	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.56.227	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3

11-05-2015-09:04:07 to 11-05-2015-10:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
132.74.56.238	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
31.168.136.9	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-05-2015-09:04:07 to 11-05-2015-10:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.166.221.34	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.255	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.106.227.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
119.73.228.136	147.237.76.42	Singapore	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.128.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
5.29.202.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.193.160.234	147.237.8.46	Russian Federation	e.chinuch.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
119.73.228.136	147.237.76.42	Singapore	refuah.idf.il	ET SCAN NMAP -sS window 4096	1

11-05-2015-09:04:07 to 11-05-2015-10:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2106
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	389
148.177.129.212	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	148
185.4.252.172	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	114
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
196.207.233.184	Senegal	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
37.26.146.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
195.160.240.11	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	63
2.54.62.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
2.52.53.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
31.168.100.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
148.177.129.210	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
77.158.88.42	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
213.204.127.27	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
66.249.65.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
58.178.197.178	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
213.6.64.134	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
79.182.114.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
199.203.215.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
46.19.85.133	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	34
192.114.23.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
37.26.148.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
2.52.131.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
2.54.134.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
66.249.65.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
37.26.146.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
77.125.88.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.19.86.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
31.168.29.225	Israel	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
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
87.69.184.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
84.94.164.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
82.102.136.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.176.213.80	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
192.118.11.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
62.105.140.248	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.86.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23

11-05-2015-09:04:07 to 11-05-2015-10:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	141
176.13.18.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
2.54.162.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
87.68.33.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	8
87.68.33.217	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	8
194.90.25.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.146.248	Israel	147.237.76.39	mobile.meitav.idf.il	Cookie Tampering on cookie .ASPNETAUTH: Expected 01022C072FFDB6E5D208FE2C7F70C8B9E5D2080009330031003400390031003600350037003800000012F00FF, Observed 0102E09E02FCB6E5D208FEE01644C7B9E5D2080009330031003400390031003600350037003800000012F00FF	None	4
176.12.140.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.65.144.170	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
109.65.144.170	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	3
176.13.3.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.44.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	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
79.176.133.170	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.65.83	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	2
37.26.149.201	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.64.112.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.69.133.68	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter 55594cf0 in aka.idf.il/giyus/	None	1
50.63.197.201	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
5.77.53.149	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
132.76.50.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.79.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
46.19.85.8	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.64.136.124	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.174.237	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 2.52.174.237 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
5.102.254.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
89.248.128.156	Netherlands	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatusDay in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.79.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
2.52.174.237	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
66.249.67.190	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/441-he/patzar.aspx	Block	1
5.135.144.131	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
176.12.150.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.172.50.77	Israel	147.237.72.166	aka.idf.il	Too Many Cookies in a Request - 113 cookies	Block	1
66.249.79.225	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
195.160.240.11	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.19.85.164	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
81.218.33.77	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/sip_storage/files/3/1773.jpg	Block	1
66.249.79.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.230.93.232	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
2.52.36.89	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.93.233	Israel	147.237.77.176	matpash.idf.il	Distributed URL is Above Root Directory	Block	1
217.31.48.30	Czech Republic	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/rom-0	Block	1
2.54.166.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.66.38.50	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.79.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1

11-05-2015-09:04:07 to 11-05-2015-10:04:07