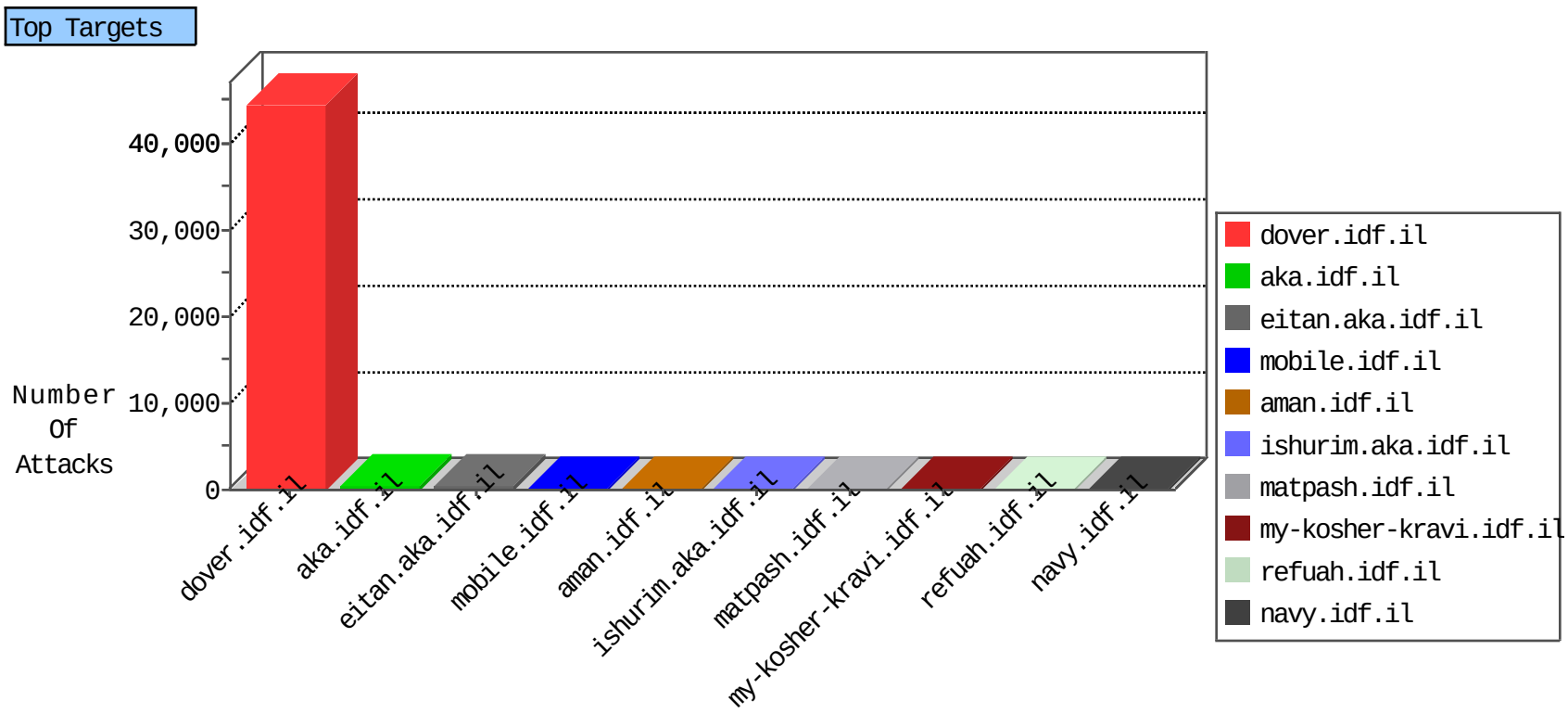
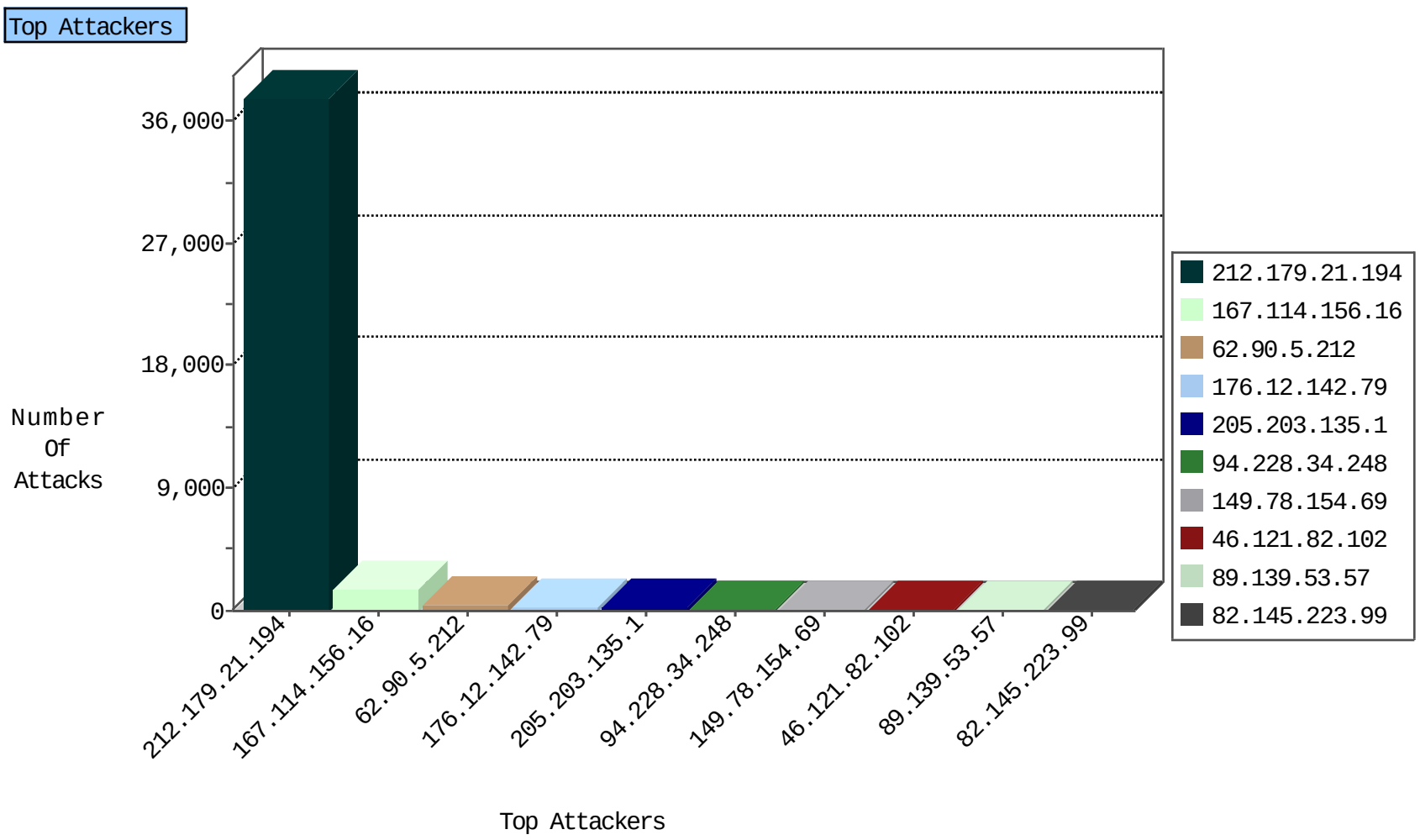
11-02-2015-17:04:04 to 11-02-2015-18:04:04

IDF Under Attack Daily Report





11-02-2015-17:04:04 to 11-02-2015-18:04:04

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	2927
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	102
212.235.98.139	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	83
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	26
62.0.84.78	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
62.219.140.28	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	15
176.13.10.151	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
62.0.84.78	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
85.64.234.158	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.180.127.76	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
84.108.62.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.183.26.96	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
109.64.147.50	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
212.199.107.106	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
93.173.247.53	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
37.142.68.89	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.94.164.85	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.46	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.176.131.229	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
185.27.105.136	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.18.232	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
31.168.227.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.51.225	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.142.68.19	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
89.46.182.7	Romania	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
90.191.209.134	Estonia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
201.52.151.16	Brazil	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
37.142.68.43	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.17.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.86.123	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
66.249.78.227	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
212.179.155.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.51.225	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
94.102.52.213	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
82.166.247.66	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
10.0.0.14		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
176.12.140.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
185.115.124.16		147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
109.64.60.233	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.86.123	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.183.155.79	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
198.48.92.104	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
183.60.48.25	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
81.218.97.114	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.85.84	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

11-02-2015-17:04:04 to 11-02-2015-18:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.188.46	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-02-2015-17:04:04 to 11-02-2015-18:04:04

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	4
66.249.67.6	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
79.180.127.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.237.109.31	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.76.202	United States	e.halag.idf.il	ET DROP Dshield Block Listed Source	1
109.66.14.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
107.2.79.150	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
103.17.55.55	147.237.0.19	Indonesia	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.12	147.237.72.156		aman.idf.il	portscan: TCP Distributed Portscan	1
107.2.79.150	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
107.2.79.150	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -f -sS	1

11-02-2015-17:04:04 to 11-02-2015-18:04:04

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	37719
62.90.5.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	392
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	167
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	133
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	131
82.145.223.99	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
173.220.141.227	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
89.139.53.57	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
2.54.134.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
204.184.109.252	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
79.180.127.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
46.121.82.102	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	56
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
149.78.78.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
109.160.216.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
37.26.148.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
212.143.222.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
79.183.155.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
37.142.68.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
2.54.130.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
100.100.43.54		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36
37.26.148.170	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36
37.26.149.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
213.57.138.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	34
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
46.19.85.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
100.100.38.118		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	28
41.188.125.185	Mauritania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
138.134.102.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
212.179.21.194	Israel	147.237.0.16	my-kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
79.178.112.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
87.68.49.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
62.219.140.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
207.46.13.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
213.57.132.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	26
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
41.237.109.31	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23

11-02-2015-17:04:04 to 11-02-2015-18:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.142.79	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	194
46.121.82.102	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
89.139.53.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
46.19.85.57	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.192	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.21	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.12.149.150	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
85.250.42.116	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
109.186.144.171	Israel	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	2
85.250.42.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	2
37.26.148.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.17.9	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
109.186.144.171	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/ajax/updatestatus.php	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
85.250.42.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
87.69.86.21	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
77.125.9.161	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.138.8	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
87.69.86.21	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	2
176.13.1.16	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.1.16	None	1
79.181.223.142	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
41.237.109.31	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/	Block	1
109.67.138.147	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
79.177.15.234	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
5.29.46.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	1
89.139.19.105	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 89.139.19.105	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
212.199.57.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.21.27	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
46.19.86.64	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.192.151	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
37.26.147.136	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
93.173.27.14	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.54.165.46	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
87.68.16.119	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/ajax/updatestatus.php	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
176.13.8.169	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.182.6.64	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.4	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.177.25.29	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	1
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.29.46.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
89.139.19.105	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/resources/images/	Block	1
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/72023-he/maarachot.aspx	Block	1
213.57.158.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

11-02-2015-17:04:04 to 11-02-2015-18:04:04