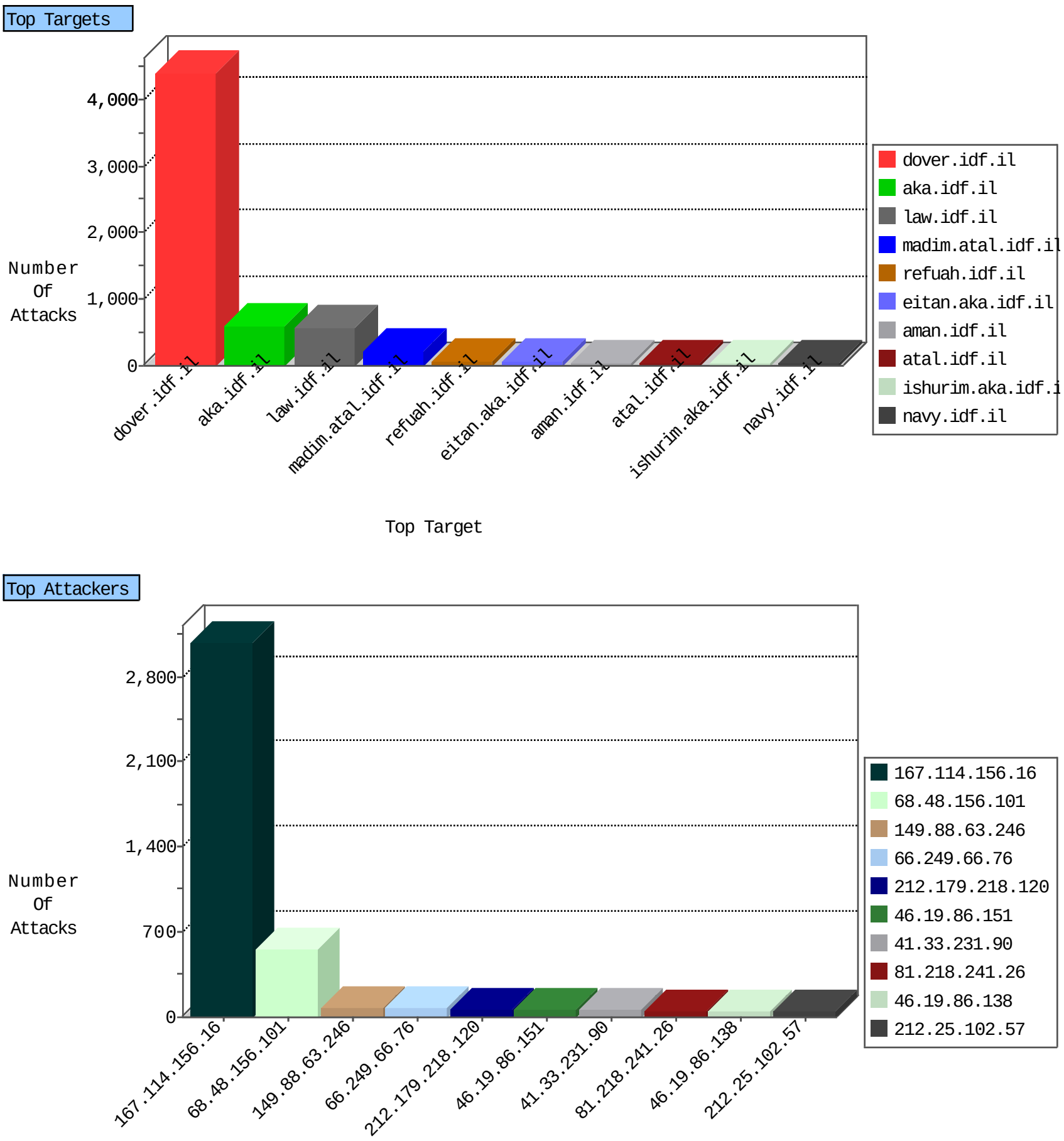
11-23-2015-16:04:08 to 11-23-2015-17:04:08

IDF Under Attack Daily Report



11-23-2015-16:04:08 to 11-23-2015-17:04:08

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	1197
66.249.78.82	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	414
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
46.48.73.60	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	3
79.177.146.167	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
192.116.199.98	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
92.252.132.80	Russian Federation	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
46.166.188.68	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

11-23-2015-16:04:08 to 11-23-2015-17:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.154.75.29	Morocco	147.237.77.216	dover.idf.i	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
24.220.5.234	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
167.114.156.16	Canada	147.237.77.216	dover.idf.i	8262: HTTP: Slowloris DoS Tool	Block	1
51.254.131.245	United Kingdom	147.237.77.216	dover.idf.i	C1000106: HTTP: majestic bot	Block	1
68.48.156.101	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
68.48.156.101	United States	147.237.77.74	law.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1

11-23-2015-16:04:08 to 11-23-2015-17:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
68.48.156.101	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	551
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
176.13.12.19	147.237.76.42	Israel	refuah.idf.il	INDICATOR-SCAN myscan	2
176.13.12.19	147.237.76.42	Israel	refuah.idf.il	GPL SCAN myscan	2
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
109.186.180.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.194.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.210.24	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
74.208.43.251	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
46.120.227.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.80.155.223	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
114.35.199.5	147.237.76.38	Taiwan	e.e.meitav.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.66.185.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.166.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.99.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
195.244.23.42	147.237.77.74	Israel	law.idf.il	ET SCAN NMAP -sA (2)	1

11-23-2015-16:04:08 to 11-23-2015-17:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2524
149.88.63.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
66.249.66.76	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52
31.186.228.31	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
31.186.228.32	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
31.186.228.58	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
79.182.144.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
31.186.228.57	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
31.186.228.30	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
37.26.148.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
100.100.57.201		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
31.186.228.94	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
105.233.74.140	South Africa	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
31.186.228.59	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
213.24.134.133	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
109.65.133.101	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
212.179.218.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
80.98.110.169	Hungary	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
212.179.218.120	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
31.186.228.93	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
212.179.218.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
192.116.199.98	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
213.57.142.2	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
31.186.228.60	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
212.179.221.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
37.26.148.231	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	12
100.100.103.32		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
100.100.8.228		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
31.186.228.95	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.65.213.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.77.167.0	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
85.130.221.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.66.79	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
66.249.66.76	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.54.63.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
213.57.134.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
37.26.148.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10

11-23-2015-16:04:08 to 11-23-2015-17:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
46.19.86.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
2.52.130.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	37
37.26.148.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
164.138.113.149	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 164.138.113.149	Block	8
46.19.86.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
37.142.64.55	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
213.57.53.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	4
176.12.144.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	3
149.78.67.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.239	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.87.164	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
82.81.160.227	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
81.218.101.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
89.202.105.211	Germany	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
79.180.207.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.1.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.121.198.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
140.101.20.1	United States	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.13.3.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.116.199.98	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.66.119	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18590-he/dover.aspx	Block	1
109.66.166.230	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
46.19.85.107	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res ources/images/innerpage/goback.gif	Block	1
79.181.59.15	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
176.13.3.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.130.139.129	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
212.179.221.203	Israel	147.237.72.166	aka.idf.il	Web leech 9	Block	1
2.52.38.193	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/images/shared/home.png	Block	1
77.125.146.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.89.56	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
82.81.160.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.93.203	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.64.195	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.65.165.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
79.181.59.15	Israel	147.237.77.216	dover.idf.il	NULL Character in Method [[#23]][[#3]][[#3]][[#0]]([[#14]]Ã?Ã?[[#8]]Â»ÂƒYSÂ.ÃµÂ¤Ã£	Block	1
188.120.148.228	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized Method POST for www.chinuch.aka.idf.il/900-he/chinuch.aspx	None	1
176.12.147.202	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 176.12.147.202	Block	1
46.121.26.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

11-23-2015-16:04:08 to 11-23-2015-17:04:08