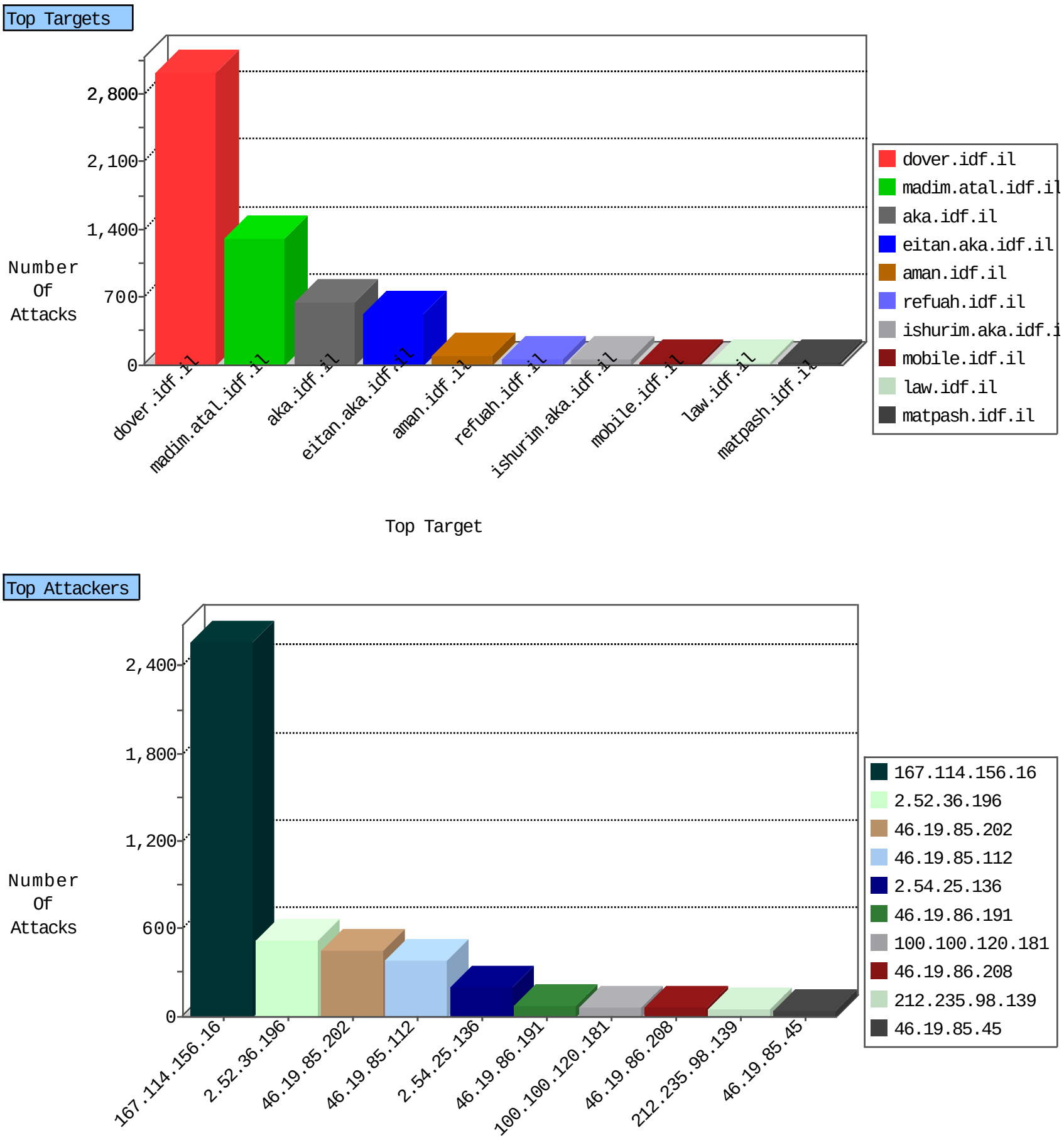
11-30-2015-12:04:00 to 11-30-2015-13:04:00

IDF Under Attack Daily Report



11-30-2015-12:04:00 to 11-30-2015-13:04:00

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	3449
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
158.169.150.8	Belgium	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	7
185.35.62.219	Switzerland	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
185.35.62.222	Switzerland	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

11-30-2015-12:04:00 to 11-30-2015-13:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
111.206.116.217	China	147.237.0.17	m.my-kosher-kravi.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
111.206.116.217	China	147.237.0.19	madim.atal.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
178.209.120.50	Russian Federation	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

11-30-2015-12:04:00 to 11-30-2015-13:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.45	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	17
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	2
79.138.70.153	147.237.76.198	Sweden	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
51.254.46.129	147.237.8.45	United Kingdom	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.54.42.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.70.66.13	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
98.239.31.233	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.198.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.20.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.138.70.153	147.237.76.199	Sweden	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.76.176	Sweden	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.117.138.210	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.6.71.154	147.237.8.50	Poland	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
162.248.54.64	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.160.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.118.63	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.118.126	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.17.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

11-30-2015-12:04:00 to 11-30-2015-13:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.36.196	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	471
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	52
2.54.12.239	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	35
100.100.120.181		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
31.168.89.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
80.246.133.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
141.0.14.34	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
212.199.244.112	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	22
100.100.120.181		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	21
2.52.134.26	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
46.19.86.193	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	20
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
62.219.112.162	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
158.169.150.8	Belgium	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	13
100.100.39.184		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
2.52.164.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.39.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.234	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
95.35.85.67	Israel	147.237.77.212	e.dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
84.94.111.49	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
2.54.41.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
100.100.120.181		147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	10
46.19.85.5	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
100.100.58.198		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.176.192.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.176.192.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
64.233.172.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
2.54.50.198	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.50.198	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	8
93.172.96.230	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
65.49.14.76	Anonymous Proxy	147.237.72.166	aka.idf.il	drop		drop	8
2.54.42.197	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
173.252.88.244	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
100.100.70.144		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.54.129.244	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.52.134.26	Israel	147.237.72.156	aman.idf.il	SYN Attack		reject	7
62.0.200.198	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer (no data). Urgent data indication was stripped. Please refer to sk36869.	drop	6
213.0.52.213	Spain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.133.212	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.64.178.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
64.233.172.163	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.137.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
66.249.69.34	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

11-30-2015-12:04:00 to 11-30-2015-13:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	235
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	227
46.19.85.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	191
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	106
2.54.25.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
2.54.25.136	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.25.136	Block	95
46.19.86.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	69
46.19.86.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	57
2.52.36.196	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
176.12.142.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
46.19.85.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	24
176.13.3.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
2.54.139.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
176.12.142.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
46.19.86.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/$$$&?&?$$$	Block	6
176.13.1.101	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	6
176.12.137.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
176.13.7.68	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	4
74.220.207.112	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
88.208.205.115	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
188.65.115.210	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
69.27.107.54	Canada	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
182.160.163.148	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
176.13.14.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.146.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.134.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
27.50.90.106	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
80.246.136.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
209.88.173.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/$$$&?&?$$$	Block	3
162.243.140.82	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
27.50.90.106	Australia	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
118.127.32.136	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
46.32.254.74	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
74.220.207.162	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
46.19.86.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.108.33.135	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
162.243.140.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
118.127.32.136	Australia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 118.127.32.136	Block	2
81.7.14.25	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
182.160.163.148	Australia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
176.13.23.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
27.50.90.106	Australia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
46.32.254.74	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
74.220.207.162	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
46.19.86.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
162.243.140.82	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
46.19.86.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2

11-30-2015-12:04:00 to 11-30-2015-13:04:00