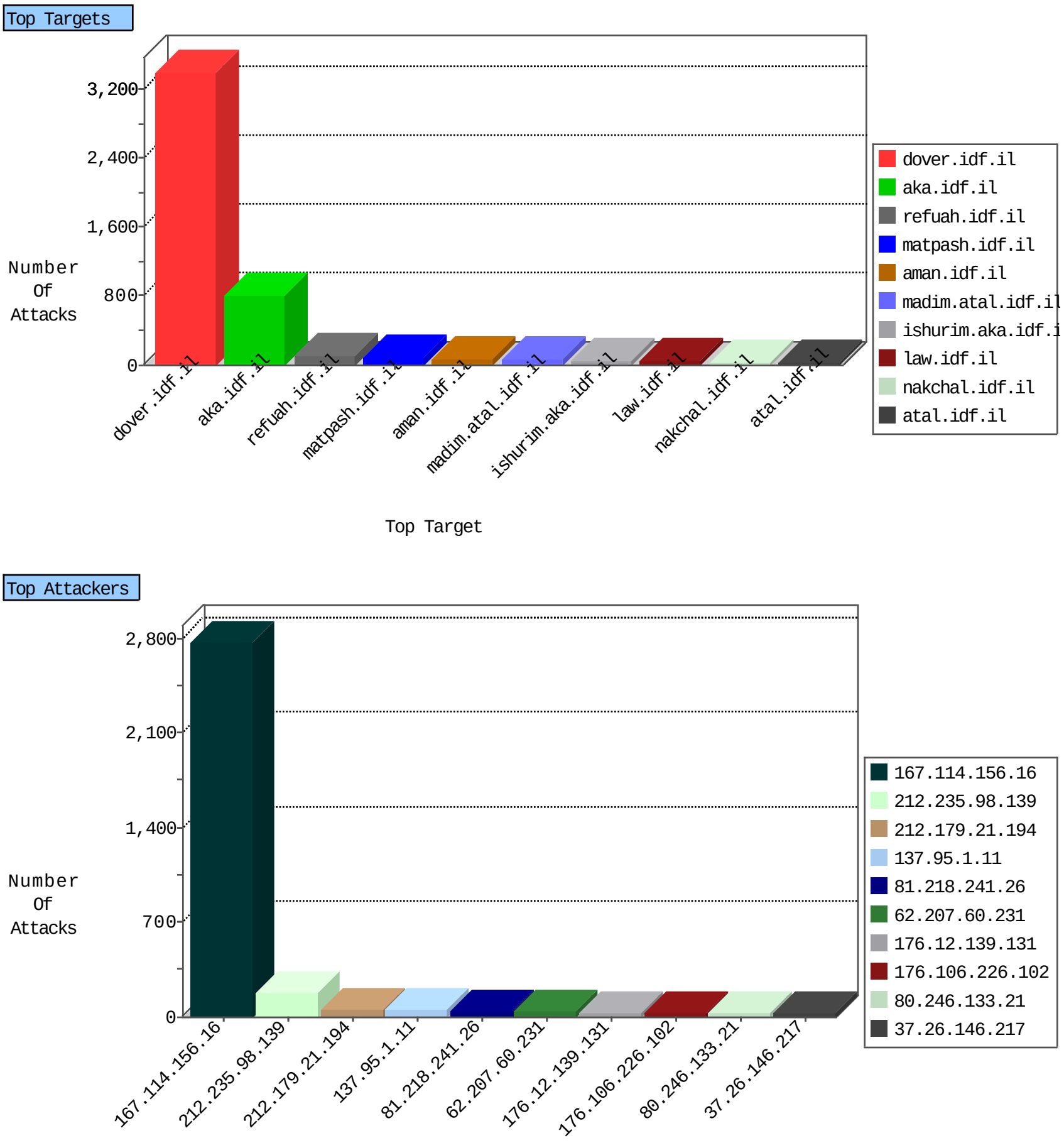
12-01-2015-11:04:02 to 12-01-2015-12:04:02

IDF Under Attack Daily Report



12-01-2015-11:04:02 to 12-01-2015-12:04:02

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	3661
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3351
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3113
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	124
81.218.56.125	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
222.186.56.107	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
141.212.122.78	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.79	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
46.19.86.248	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
81.218.56.125	Israel	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1

12-01-2015-11:04:02 to 12-01-2015-12:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
161.202.41.12	Netherlands	147.237.76.42	refuah.idf.il	C003: HTTP: phpMyAdmin access	Block	1
151.80.31.143	Italy	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1
161.202.41.12	Netherlands	147.237.76.31	nakchal.idf.il	C003: HTTP: phpMyAdmin access	Block	1

12-01-2015-11:04:02 to 12-01-2015-12:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.90.76.231	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	7
183.61.109.189	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -f -sS	1
119.73.228.130	147.237.0.16	Singapore	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
91.223.208.142	147.237.72.217	Cyprus	e.idf.il	ET SCAN Potential SSH Scan	1
82.192.90.145	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential SSH Scan	1
2.54.61.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
185.3.146.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.61.109.189	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 2048	1
176.12.137.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.141.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.159.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.140.127	147.237.72.166	Israel	aka.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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
183.61.109.189	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1

12-01-2015-11:04:02 to 12-01-2015-12:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	182
137.95.1.11	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	56
62.207.60.231	Netherlands	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	38
176.12.139.131	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
80.246.133.21	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
46.19.86.115	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
212.199.218.214	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.18.33		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
93.172.183.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
212.179.21.194	Israel	147.237.0.16	my-kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
217.194.202.150	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
109.64.59.60	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
213.57.131.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
100.100.46.239		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
213.57.131.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
80.246.130.188	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.89	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
65.49.14.89	Anonymous Proxy	147.237.72.166	aka.idf.il	drop		drop	7
109.64.160.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.53.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.67.53.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.32.179.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.176.12.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.176	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
213.8.44.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.86.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.198.7	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
207.46.13.4	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.95.198.7	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.181	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
79.181.113.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.186	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.254.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.146.181	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	5
109.65.117.24	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.178.171.222	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
2.54.2.240	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.178.171.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.11	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.95.255.130	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
194.90.240.121	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	43
37.26.146.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
77.127.151.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	22
176.12.140.41	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	21
192.115.67.2	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	18
176.106.226.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
84.108.47.57	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	12
89.139.176.245	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	12
212.143.3.44	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	12
176.13.5.150	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	11
46.19.86.60	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	11
46.19.86.223	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
176.13.4.229	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
62.0.54.2	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
80.246.133.21	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	9
37.26.146.241	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
2.101.192.27	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
213.8.44.227	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
176.13.1.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
176.13.20.73	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
176.13.5.64	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
37.26.146.190	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
176.12.142.210	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
84.228.251.80	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
185.120.126.58		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
2.52.16.211	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
2.54.5.172	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
212.199.182.150	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
213.57.84.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
37.26.147.205	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
79.180.71.110	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
82.81.193.82	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
46.117.226.55	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
85.250.252.27	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
200.6.104.28	Chile	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
89.139.176.245	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
176.12.145.195	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
93.172.28.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
60.241.215.85	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
185.120.126.58		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
108.59.253.71	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
83.170.118.9	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
2.54.172.28	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.12.149.197	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.90.106	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3

12-01-2015-11:04:02 to 12-01-2015-12:04:02