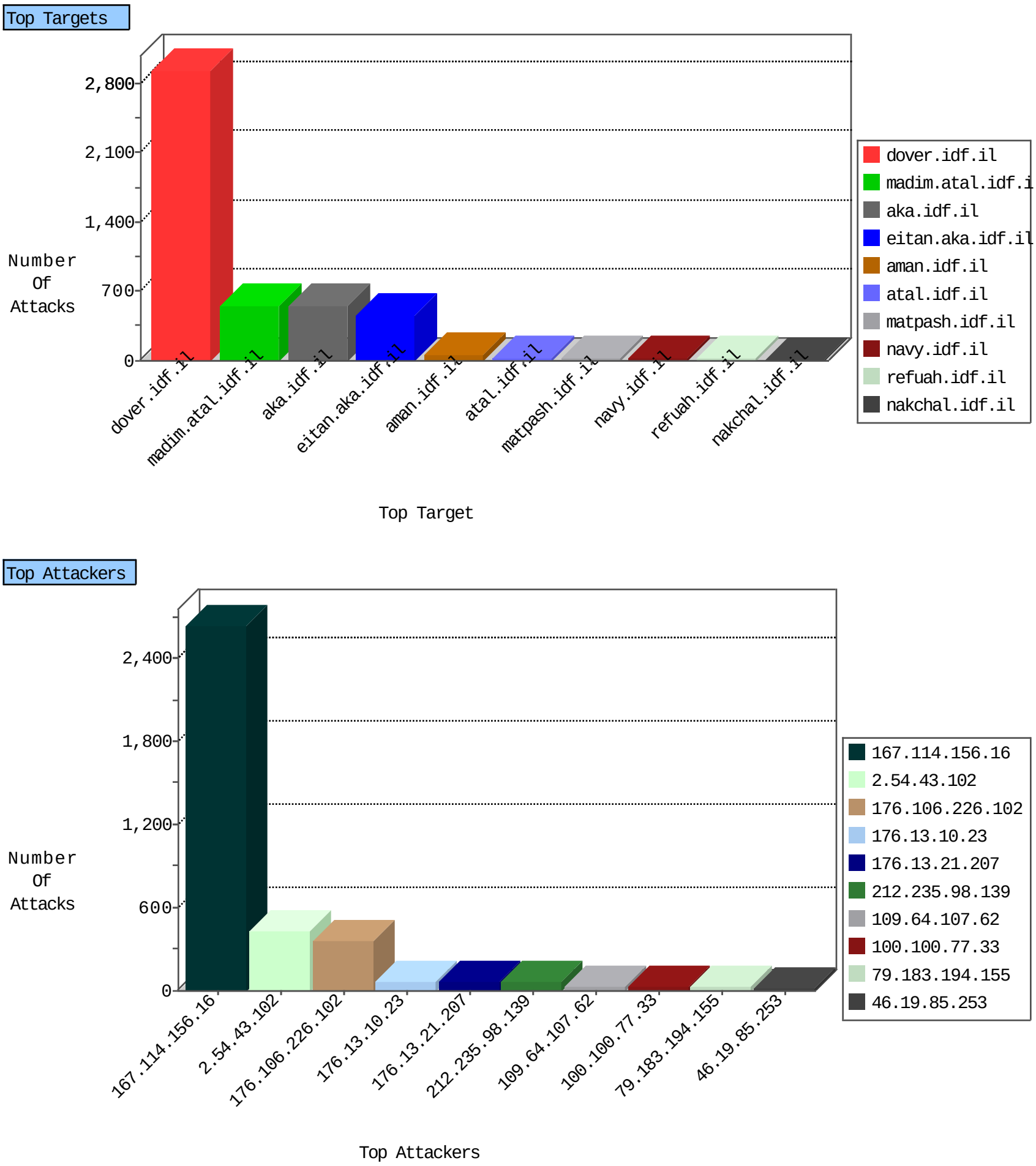
12-01-2015-12:04:06 to 12-01-2015-13:04:06

IDF Under Attack Daily Report



12-01-2015-12:04:06 to 12-01-2015-13:04:06

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	3484
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	189
66.249.66.1	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	72
109.64.107.62	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	9
109.64.107.62	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
204.42.253.130	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
94.102.49.210	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
81.218.56.125	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.210	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

12-01-2015-12:04:06 to 12-01-2015-13:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-01-2015-12:04:06 to 12-01-2015-13:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.149	147.237.0.19	Israel	madim.atal.idf.i	POLICY-OTHER TCP packet with urgent flag attempt	8
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
109.66.11.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.211.117.83	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	1
84.228.225.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.67.132	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
5.102.214.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.245.240.26	147.237.76.200	Australia	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
137.44.1.153	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
95.211.117.83	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
93.173.0.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.50.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.40.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
42.48.224.76	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.26.146.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.245.240.26	147.237.76.200	Australia	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
149.78.248.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-01-2015-12:04:06 to 12-01-2015-13:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.43.102	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	405
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	61
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
79.183.194.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.18.33		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
109.64.107.62	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
81.218.131.98	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.55.253	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
100.100.49.151		147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	8
192.117.167.66	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
213.57.136.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
65.49.14.89	Anonymous Proxy	147.237.72.166	aka.idf.il	drop		drop	7
213.57.130.70	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
213.57.130.70	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
213.57.136.177	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.117.167.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.73	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.6.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.157.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.28	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.179.183.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.139.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.73	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.75.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
199.203.226.21	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.108.118.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
94.230.86.146	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.136.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.145.211	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.94	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.247	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.125.94.22	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
207.46.13.91	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.28	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.229.107.7	United Kingdom	147.237.77.216	dover.idf.il	drop	SAM rule	drop	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

12-01-2015-12:04:06 to 12-01-2015-13:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.106.226.102	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.106.226.102	Block	202
176.106.226.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
176.13.10.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
176.106.226.102	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.106.226.102	Block	67
176.13.21.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
2.54.43.102	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	27
176.13.3.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
2.52.49.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
82.166.219.13	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	5
149.88.58.140	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.88.58.140	Block	4
46.120.233.241	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.233.241	Block	4
79.177.104.171	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
173.254.55.58	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
46.19.85.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
173.254.24.31	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
111.235.136.184	Singapore	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
178.32.28.117	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
221.121.151.95	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
5.61.249.41	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
186.202.127.240	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
212.25.84.200	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	3
46.19.85.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
206.214.223.200	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
138.128.182.90	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
104.236.117.177		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
173.255.139.12	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
111.235.136.184	Singapore	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
178.32.28.117	France	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
221.121.151.95	Australia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
138.128.182.90	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
5.61.249.41	Netherlands	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
176.12.150.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
173.254.55.58	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 173.254.55.58	Block	2
46.19.86.110	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
186.202.127.240	Brazil	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
104.236.117.177		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
82.166.219.13	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.166.219.13	Block	2
46.19.86.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
173.254.24.31	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 173.254.24.31	Block	2
206.214.223.200	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
81.218.131.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
138.128.182.90	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	2
178.32.28.117	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.32.28.117	Block	2
104.236.117.177		147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
173.255.139.12	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	2
213.57.175.93	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
176.13.15.142	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2

12-01-2015-12:04:06 to 12-01-2015-13:04:06