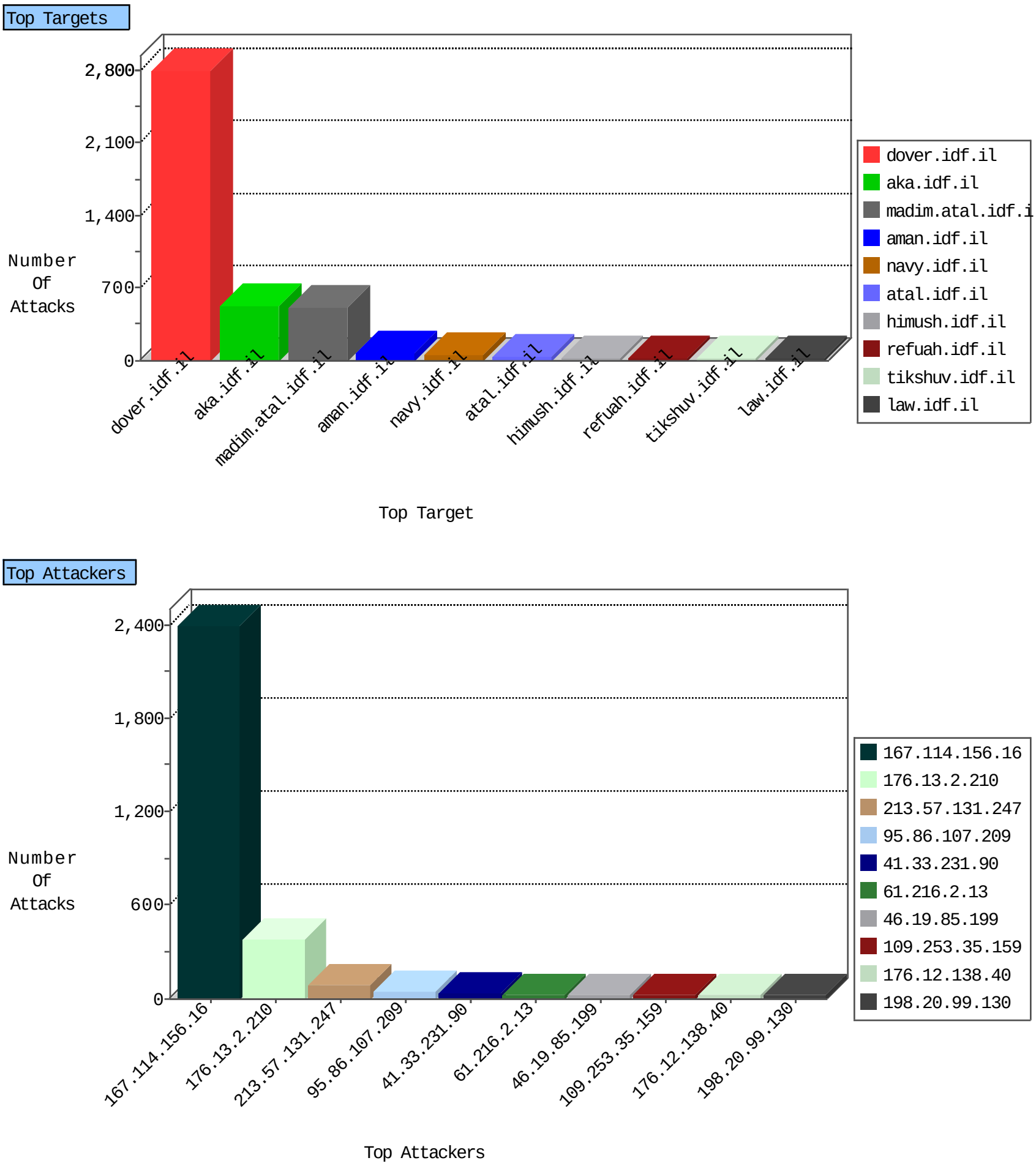
12-01-2015-17:04:03 to 12-01-2015-18:04:03

IDF Under Attack Daily Report



12-01-2015-17:04:03 to 12-01-2015-18:04:03

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	3248
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2959
198.20.99.130	Netherlands	147.237.76.30	himush.idf.il	TCP Scan (vertical)	drop	133
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	56
198.20.99.130	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	6
79.178.108.146	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
80.246.137.222	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	6
198.20.99.130	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	5
198.20.99.130	Netherlands	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
71.6.165.200	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
89.163.140.142	Germany	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.151	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
82.80.162.39	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
198.20.99.130	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

12-01-2015-17:04:03 to 12-01-2015-18:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-01-2015-17:04:03 to 12-01-2015-18:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.250.148.225	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
91.201.236.113	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -sS window 1024	1
72.222.110.28	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
222.124.109.131	147.237.77.216	Indonesia	dover.idf.il	ET SCAN Potential SSH Scan	1
2.54.158.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.124.109.131	147.237.76.31	Indonesia	nakchal.idf.il	ET SCAN Potential SSH Scan	1
222.124.109.131	147.237.72.167	Indonesia	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.48.195	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.67.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.118.11.140	147.237.77.216	Romania	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.89.108	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	1
222.124.109.131	147.237.77.170	Indonesia	maarachot.idf.il	ET SCAN Potential SSH Scan	1
222.124.109.131	147.237.72.217	Indonesia	e.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

12-01-2015-17:04:03 to 12-01-2015-18:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	28
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	28
100.100.120.227		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
85.65.79.222	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	16
82.80.175.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
80.250.148.225	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
100.100.84.97		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
100.100.56.63		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
100.100.59.141		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
66.249.75.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.11.161		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
37.26.148.196	Israel	147.237.0.34	tikshuv.idf.i	drop	First packet isn't SYN	drop	11
213.57.131.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
2.54.137.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
37.201.169.150	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.47	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
213.57.131.247	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.27.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.147	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.146.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.23.133		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
5.22.134.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.176.158.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.211.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.8.114.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.114.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.142.101.217	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.109.50.161	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.137.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.131.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5

12-01-2015-17:04:03 to 12-01-2015-18:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.2.210	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.2.210	Block	185
176.13.2.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
176.13.2.210	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.2.210	Block	91
95.86.107.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
176.12.138.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
176.12.147.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
176.13.21.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
176.12.148.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.6.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
95.35.169.97	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6
176.28.17.231	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.28.17.231	Block	5
176.13.0.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.128.185	Block	3
23.235.194.89	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
210.48.70.181	New Zealand	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
176.12.136.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
216.119.129.194	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
50.87.165.17	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
157.55.39.247	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 157.55.39.247	Block	2
23.235.194.89	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
210.48.70.181	New Zealand	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
86.25.8.57	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
66.249.66.31	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	2
79.178.32.19	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
50.87.165.17	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
86.25.8.57	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	2
84.108.212.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
210.48.70.181	New Zealand	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
176.13.11.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
216.119.129.194	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
176.12.142.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.67.217.139	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
37.26.147.250	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	2
50.87.165.17	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
23.235.194.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
62.219.139.217	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/72083-he/maarachâ€‹ot.asps	Block	2
40.77.167.16	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/security/edid/signin-form	Block	1
84.108.51.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
197.35.112.68	Egypt	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
66.249.66.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/20/	Block	1
149.88.185.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.168.242.197	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.180.179.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.16.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
61.216.2.13	Taiwan	147.237.77.74	law.idf.il	Illegal Byte Code Character in Method	Block	1
109.64.199.37	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
216.119.129.194	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 216.119.129.194	Block	1
46.121.133.82	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
89.138.212.137	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1

12-01-2015-17:04:03 to 12-01-2015-18:04:03