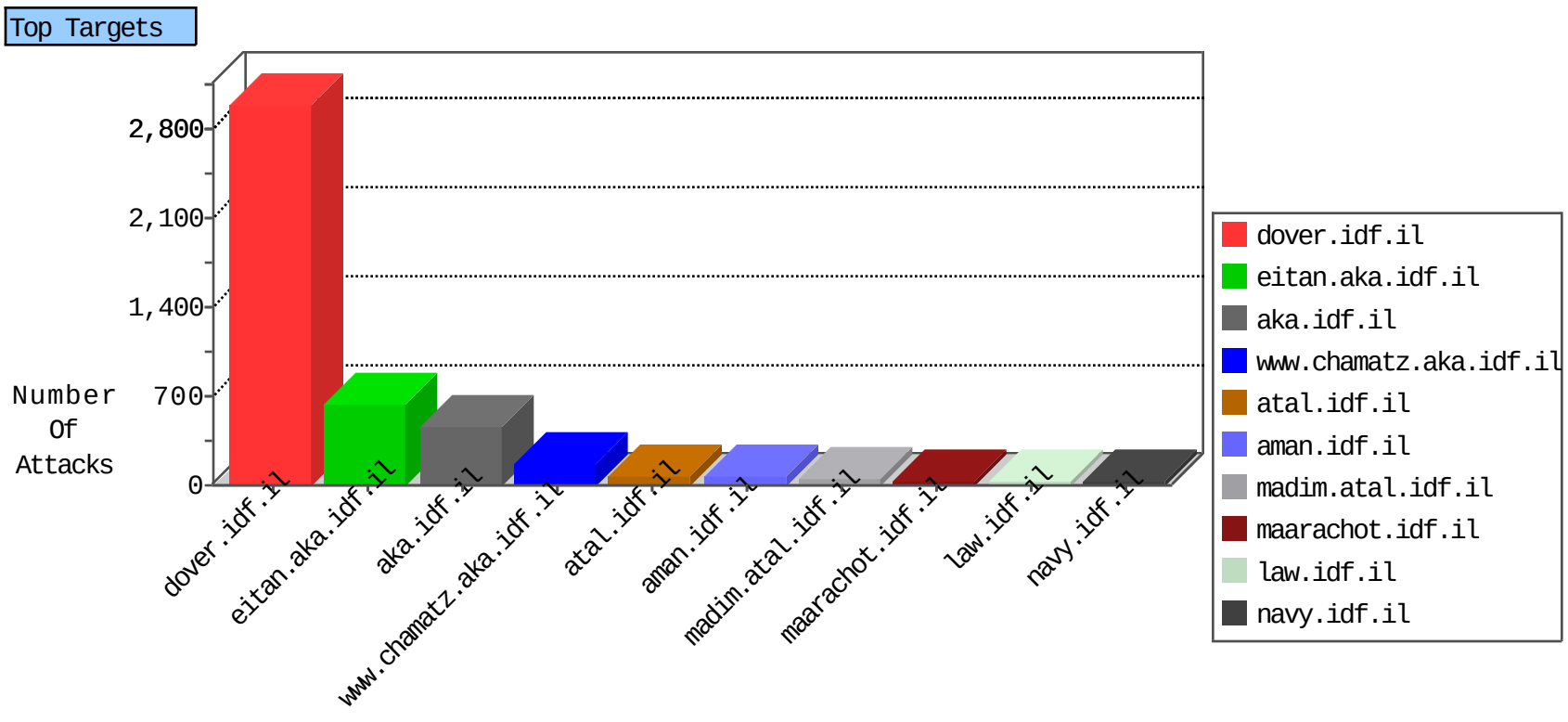
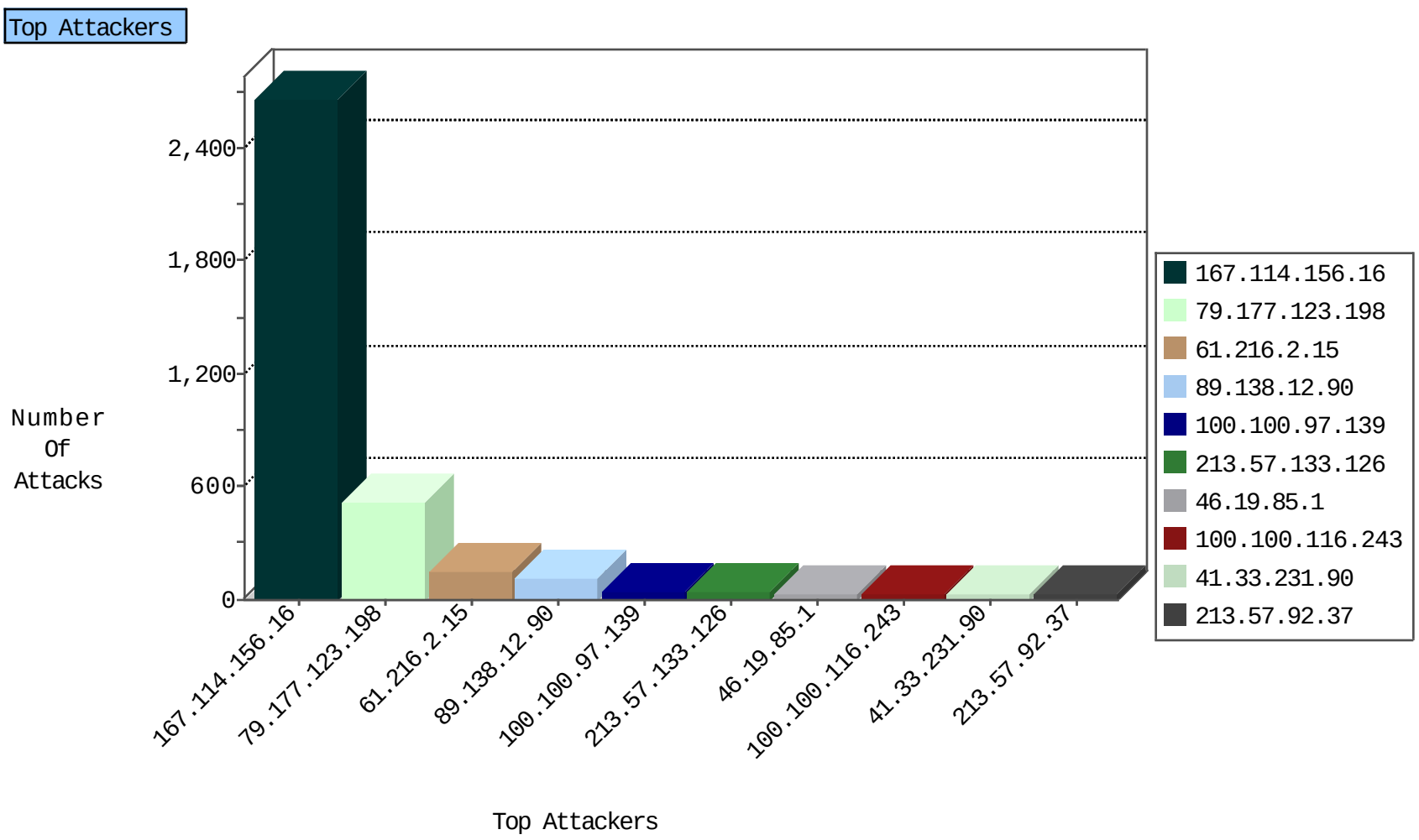
11-30-2015-23:04:03 to 12-01-2015-00:04:03

IDF Under Attack
Daily Report





11-30-2015-23:04:03 to 12-01-2015-00:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	17974
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3508
109.65.151.184	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.181.9.175	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.181.9.175	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
162.222.185.165	United States	147.237.76.147	chinuch.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
62.209.11.136	Bahrain	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
199.48.164.230	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
162.255.63.134	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
62.209.11.137	Bahrain	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
62.209.11.138	Bahrain	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
192.3.170.124	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1

11-30-2015-23:04:03 to 12-01-2015-00:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
142.4.214.124	Canada	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
183.245.117.220	China	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

11-30-2015-23:04:03 to 12-01-2015-00:04:03

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
162.222.185.165	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
162.222.185.165	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	2
117.58.247.69	147.237.77.233	Bangladesh	atal.idf.il	ET SCAN NMAP -sS window 2048	1
117.58.247.69	147.237.77.233	Bangladesh	atal.idf.il	ET SCAN NMAP -f -sS	1
98.119.105.221	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
176.12.146.56	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.131.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
162.222.185.165	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
84.109.215.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
162.222.185.165	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.27	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
117.58.247.69	147.237.77.233	Bangladesh	atal.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.155	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
176.12.149.54	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
97.105.43.174	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
85.64.255.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
162.222.185.165	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
84.109.89.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.222.185.165	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
31.154.10.107	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
162.222.185.165	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1

11-30-2015-23:04:03 to 12-01-2015-00:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.177.123.198	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	462
89.138.12.90	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	112
100.100.97.139		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	45
100.100.116.243		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
213.57.92.37	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
31.186.228.30	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	26
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
31.186.228.60	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	22
31.186.228.31	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	19
100.100.102.227		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
213.57.133.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
31.186.228.58	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	14
213.57.133.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
213.57.133.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
31.186.228.32	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	14
100.100.44.112		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.148.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.182.18.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
50.140.4.64	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
31.186.228.29	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	10
2.222.211.59	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
31.186.228.59	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	10
37.26.146.223	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
31.186.228.57	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	10
31.186.228.94	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
65.49.14.76	Anonymous Proxy	147.237.77.170	maarachot.idf.il	drop		drop	9
46.19.86.149	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
65.49.14.76	Anonymous Proxy	147.237.77.216	dover.idf.il	drop		drop	9
216.223.27.26	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	9
31.186.228.93	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	8
84.109.109.161	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
31.186.228.95	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
61.216.2.15	Taiwan	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	6
31.186.228.96	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
5.22.134.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.1	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
61.216.2.15	Taiwan	147.237.77.74	law.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	6
79.179.189.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.185	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.29.195.78	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.157	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
185.120.126.79		147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.1	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.1	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.1	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.123.198	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.177.123.198	Block	49
185.3.144.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
87.69.87.164	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	10
79.182.6.205	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/1088-he/meretz.aspx	Block	6
46.19.85.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
40.77.167.83	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/plateimage.aspx	Block	4
46.121.232.50	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	4
217.132.2.62	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-229...	Block	4
212.150.214.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
2.54.190.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
40.77.167.36	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/plateimage.aspx	Block	3
46.19.85.60	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.x in www.idf.il/1133-he/dover.aspx	Block	3
91.201.63.116	Sweden	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	3
103.26.99.147	India	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
83.145.246.174	Finland	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
2.54.142.155	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-229...	Block	3
185.11.164.16	Portugal	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
54.94.178.193	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
50.87.161.155	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	3
67.225.180.145	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
176.13.9.135	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.9.135	None	3
87.69.64.197	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
157.55.39.155	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/plateimage.aspx	Block	2
67.225.180.145	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 67.225.180.145	Block	2
91.201.63.116	Sweden	147.237.77.170	maarachot.idf.il	Distributed Admin Blocking	Block	2
54.94.178.193	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
31.210.186.138	Israel	147.237.76.86	navy.idf.il	Parameter Type Violation fromDate in www.navy.idf.il/shared/ajax/getnewslobbycontent.aspx	Block	2
103.26.99.147	India	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
50.87.161.155	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
83.145.246.174	Finland	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
185.120.126.79		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.11.164.16	Portugal	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
54.94.178.193	Brazil	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
50.87.161.155	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
67.225.180.145	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
91.201.63.116	Sweden	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/index.php	Block	2
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.51	Block	2
103.26.99.147	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
185.11.164.16	Portugal	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.11.164.16	Block	2
83.145.246.174	Finland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
2.52.43.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
61.216.2.15	Taiwan	147.237.76.42	refuah.idf.il	Multiple Illegal Byte Code Character in Method from 61.216.2.15	Block	1
93.173.128.216	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method .4 in URL	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
61.216.2.15	Taiwan	147.237.0.19	madim.atal.idf.il	Multiple Untraceable SSL Sessions from 61.216.2.15 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Unknown Parameter c@Id in www.aka.idf.il/iturim/asp/search.asp	None	1

11-30-2015-23:04:03 to 12-01-2015-00:04:03