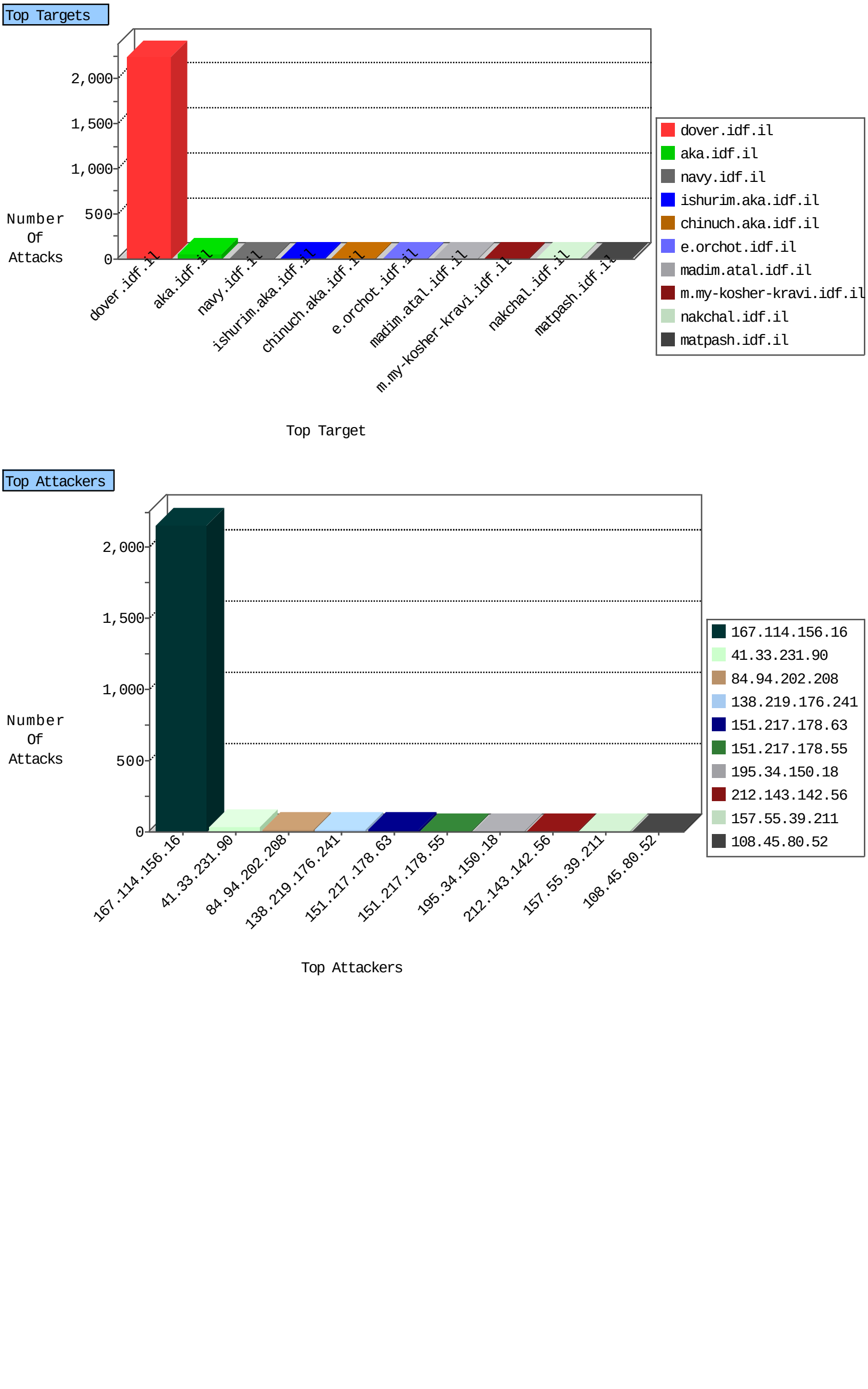
12-28-2015-05:04:05 to 12-28-2015-06:04:05

IDF Under Attack
Daily Report



12-28-2015-05:04:05 to 12-28-2015-06:04:05

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	3129
23.95.248.111	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

12-28-2015-05:04:05 to 12-28-2015-06:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-28-2015-05:04:05 to 12-28-2015-06:04:05

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
138.219.176.241	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	2
138.219.176.241	147.237.77.179		e.mazi.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.63	147.237.72.166		aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
138.219.176.241	147.237.76.201		e.atal.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.63	147.237.0.34		tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
172.98.200.238	147.237.8.24		e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
151.217.178.55	147.237.77.216		dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
138.219.176.241	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.77.61		e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
138.219.176.241	147.237.8.45		e.eitan.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.76.30		himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.68	147.237.77.205		prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
138.219.176.241	147.237.0.200		m4u.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.55	147.237.8.46		e.chinuch.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
151.217.178.63	147.237.77.170		maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
98.119.105.221	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 4096	1
151.217.178.36	147.237.77.19		law-forum.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.63	147.237.76.176		test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.82.79.41	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
151.217.176.25	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.63	147.237.76.44		e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
138.219.176.241	147.237.76.202		e.halag.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.63	147.237.8.14		e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
138.219.176.241	147.237.76.177		ncore.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.63	147.237.0.33		idf.il	ET SCAN Potential VNC Scan 5900-5920	1
138.219.176.241	147.237.76.44		e.refuah.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.77.234		halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.77.205		prisha.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
138.219.176.241	147.237.8.46		e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 1024	1
138.219.176.241	147.237.8.14		e.orchot.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.76.34		yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.63	147.237.77.235		sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
138.219.176.241	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.55	147.237.0.35		akaws.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
151.217.178.63	147.237.77.74		law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
98.119.105.221	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.176.25	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.63	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

12-28-2015-05:04:05 to 12-28-2015-06:04:05

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	36
84.94.202.208	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.23	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.247.36.122	Netherlands	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
157.55.39.211	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.53.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.146	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
37.26.147.145	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.106.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
68.180.228.112	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
2.52.6.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.26.149.146	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
141.212.122.105	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
108.2.211.152	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.36	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.103	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
45.79.168.168		147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.173	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.98	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.114	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.211	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
176.12.137.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.106	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
209.6.135.230	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.38	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.103	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
146.185.239.102	Russian Federation	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.99	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.114	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.108.77.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.212	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
70.208.6.164	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
183.206.170.123	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.187.114.171	France	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.161	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
131.253.25.185	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
209.6.135.230	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.56	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.112	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.210.158.71	Netherlands	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
37.26.147.212	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.102	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.108.77.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.247.227	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.12	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

12-28-2015-05:04:05 to 12-28-2015-06:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
108.45.80.52	United States	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	3
176.13.17.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
207.46.13.148	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.148	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
157.55.39.211	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
195.154.227.118	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
109.66.122.155	Israel	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	2
176.13.13.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.142.67	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
207.46.13.134	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
108.45.80.52	United States	147.237.77.216	dover.idf.il	Multiple Malformed URL from 108.45.80.52	Block	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
82.98.134.51	Spain	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
50.87.248.116	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
149.88.161.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
185.3.144.143	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
66.249.74.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
108.45.80.52	United States	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 108.45.80.52	Block	1
46.19.86.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
103.26.18.206	New Zealand	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
180.76.15.7	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
50.87.248.116	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
149.210.158.71	Netherlands	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 149.210.158.71	Block	1
108.2.211.152	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
207.46.13.148	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/lunxian600.asp	Block	1
77.125.86.16	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
186.202.127.23	Brazil	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
176.12.140.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
46.37.21.68	Italy	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
103.26.18.206	New Zealand	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
183.206.170.123	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/fckeditor/editor/	Block	1
66.249.66.39	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
157.55.39.1	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/1258-he/navy.aspx	Block	1
2.54.131.194	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
80.246.136.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
186.202.127.23	Brazil	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.37.21.68	Italy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
104.131.147.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
69.89.31.229	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
183.206.170.123	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/fckeditor/editor/	Block	1
66.249.66.157	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1

12-28-2015-05:04:05 to 12-28-2015-06:04:05