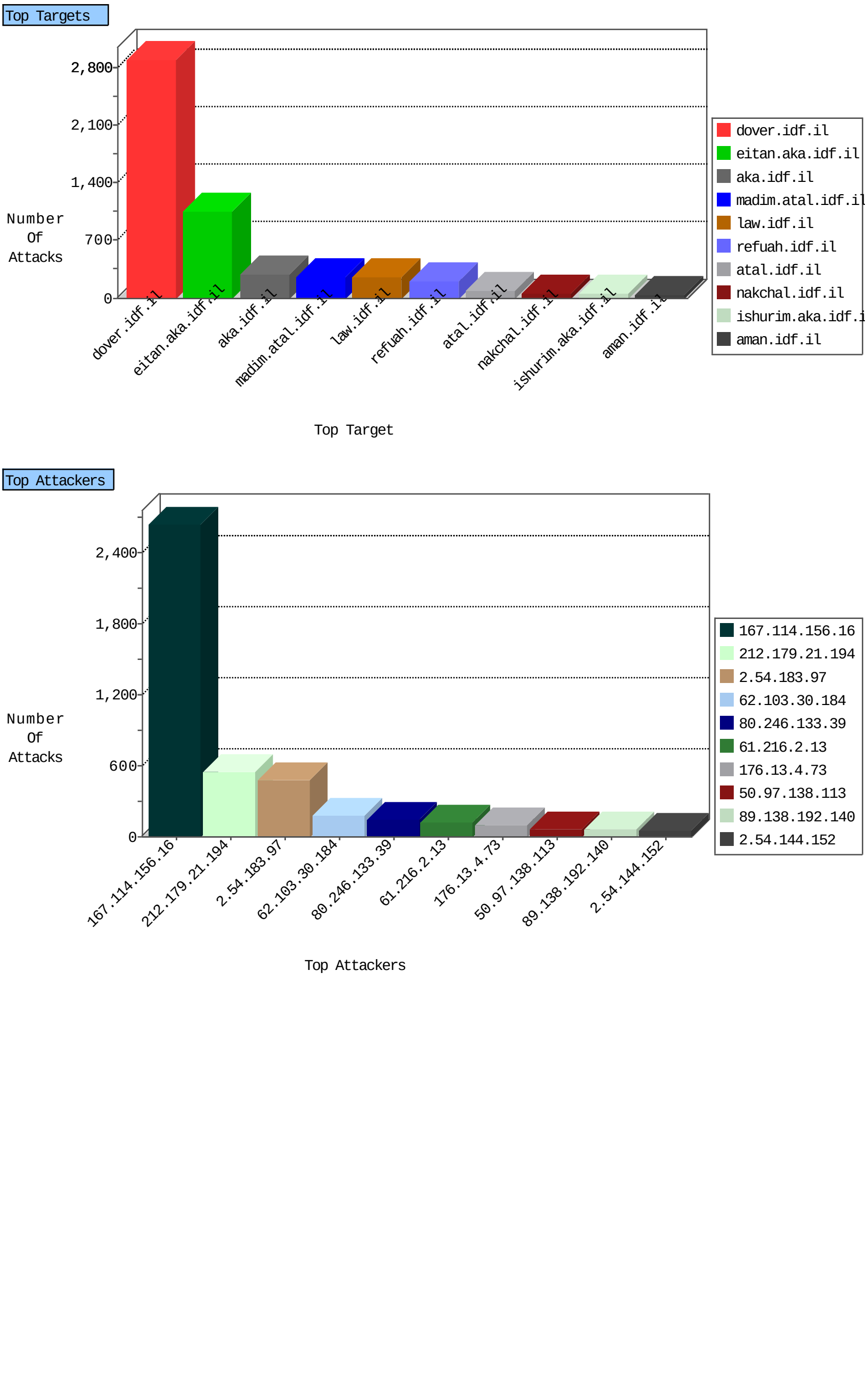
12-08-2015-16:04:01 to 12-08-2015-17:04:01

IDF Under Attack
Daily Report



12-08-2015-16:04:01 to 12-08-2015-17:04:01

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	3497
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	71
45.32.246.5		147.237.76.30	himush.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.76.31	nakchal.idf.il	Invalid TCP Flags	drop	6
84.109.12.233	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
45.32.246.5		147.237.77.61	e.cogat.idf.il	Invalid TCP Flags	drop	4
79.176.36.4	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
71.6.216.43	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
37.204.103.100	Russian Federation	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
45.32.246.5		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

12-08-2015-16:04:01 to 12-08-2015-17:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
50.97.138.113	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	14
50.97.138.113	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
50.97.138.113	United States	147.237.77.233	atal.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	2

12-08-2015-16:04:01 to 12-08-2015-17:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
50.97.138.113	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	43
66.249.88.46	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
137.226.113.7	147.237.77.234	Germany	halag.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1
109.65.148.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.126.220.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.32.246.5	147.237.77.61		e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
45.32.246.5	147.237.77.61		e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.246.5	147.237.76.31		nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
183.60.252.84	147.237.76.198	China	e.yohalan.idf.i	ET SCAN NMAP -sS window 4096	1
5.29.158.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.0.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.228.187.126	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
45.32.246.5	147.237.77.61		e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
45.32.246.5	147.237.77.61		e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
45.32.246.5	147.237.77.61		e.cogat.idf.il	ET SCAN NMAP -f -sS	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
45.32.246.5	147.237.76.31		nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
168.235.197.238	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1

12-08-2015-16:04:01 to 12-08-2015-17:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.183.97	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	441
62.103.30.184	Greece	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	178
80.246.133.39	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	141
66.249.64.70	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
212.179.21.194	Israel	147.237.77.235	sviva.idf.il	drop	First packet isn't SYN	drop	23
80.178.150.201	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
2.54.177.216	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
46.19.86.146	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
80.178.150.219	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
45.32.246.5		147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
61.216.2.13	Taiwan	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
61.216.2.13	Taiwan	147.237.77.170	maarachot.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
213.57.133.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
61.216.2.13	Taiwan	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
61.216.2.14	Taiwan	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
61.216.2.13	Taiwan	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
213.57.133.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
82.81.26.69	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
81.218.193.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
46.19.85.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.46.39.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.66.0.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
213.57.130.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
213.57.130.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.152	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
77.126.99.5	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
61.216.2.14	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
77.125.87.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.179.5.168	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
79.180.160.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.168.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.0	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.87.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.140	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
109.65.139.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.109.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.13.109.118	Ireland	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.140	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
81.218.193.205	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
109.65.139.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.23.212	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
61.216.2.13	Taiwan	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	6

12-08-2015-16:04:01 to 12-08-2015-17:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	508
176.13.4.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
89.138.192.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
2.54.144.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
2.54.183.97	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
46.19.86.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	19
2.52.13.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.109.114.79	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	5
84.109.114.79	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.109.114.79	Block	4
149.78.151.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.9.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.18.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.54.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.21.194	Israel	147.237.77.235	sviva.idf.il	Unauthorized URL Access to www.hagnas.atal.idf.il/sip_storage/files/2/1552.jpg	Block	2
84.94.39.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
149.88.206.49	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1437-he/atal.aspx	Block	2
176.13.19.16	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
2.52.148.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.81.18.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
61.216.2.13	Taiwan	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method	Block	1
173.252.121.118	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.162.80	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.29.246.67	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1334-he/refuah.aspx	Block	1
61.216.2.13	Taiwan	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
141.212.121.176	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/71552.pdf	Block	1
185.32.179.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
61.216.2.13	Taiwan	147.237.77.243	mobile.idf.il	Multiple Untraceable SSL Sessions from 61.216.2.13 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
5.22.134.52	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
61.216.2.13	Taiwan	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 61.216.2.13	Block	1
157.55.39.145	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.180.207.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9180-he/refuah.aspx	Block	1
109.160.217.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
61.216.2.14	Taiwan	147.237.76.86	navy.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
183.15.5.73	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
37.26.148.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.173.128.150	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
82.81.26.69	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
61.216.2.13	Taiwan	147.237.76.200	eitan.aka.idf.il	Illegal Byte Code Character in Method	Block	1
173.252.121.119	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
61.216.2.13	Taiwan	147.237.0.19	madim.atal.idf.il	Multiple Illegal Byte Code Character in Method from 61.216.2.13	Block	1
79.176.145.176	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.76.123.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method ana in URL	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1

12-08-2015-16:04:01 to 12-08-2015-17:04:01