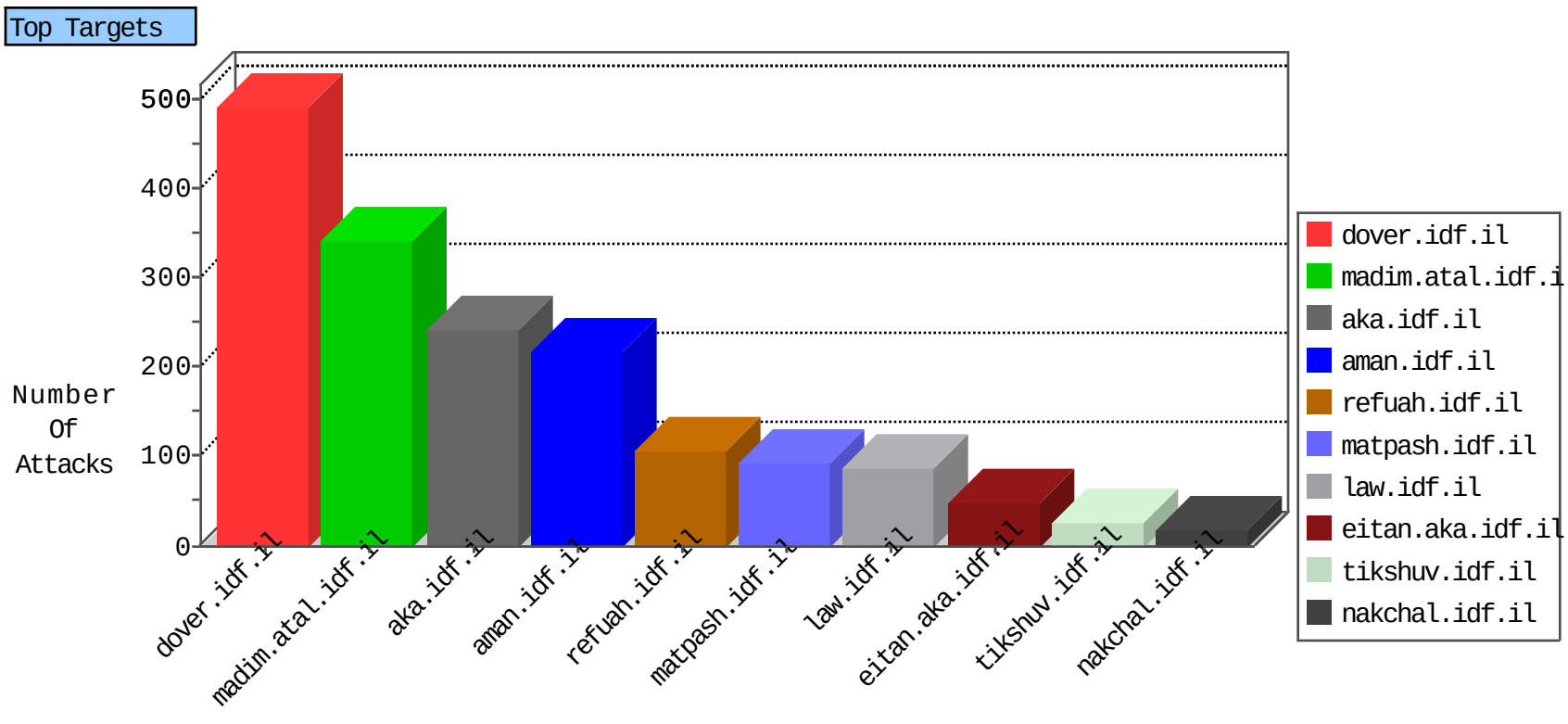
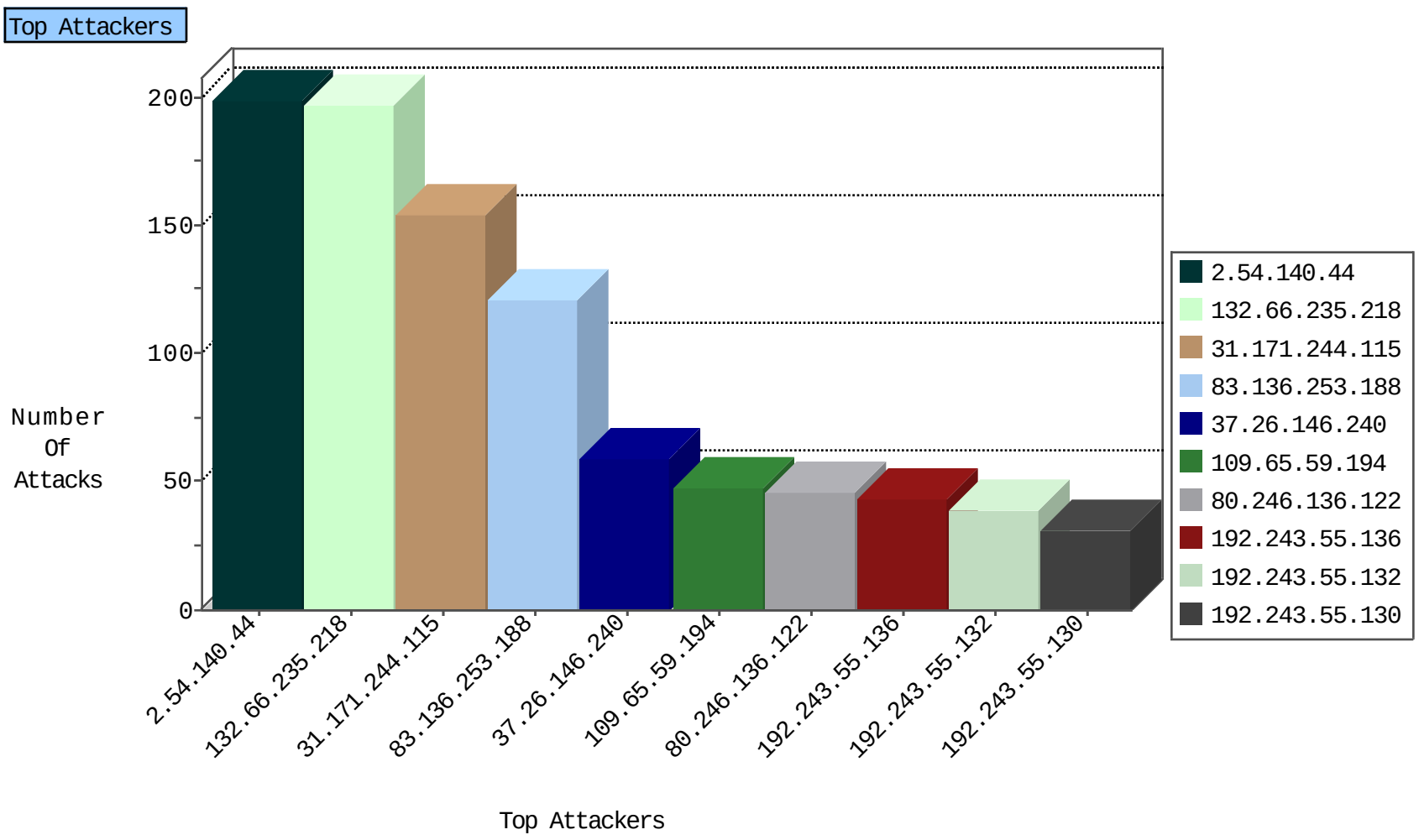
03-09-2016-13:04:08 to 03-09-2016-14:04:08

IDF Under Attack
Daily Report





03-09-2016-13:04:08 to 03-09-2016-14:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	134
82.145.222.87	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	20
82.145.209.28	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
82.145.222.189	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
93.174.93.218	Netherlands	147.237.77.74	law.idf.il	block-sp-traf1	forward	2
49.129.221.206	Japan	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
202.58.8.231	Singapore	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
87.69.229.113	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

03-09-2016-13:04:08 to 03-09-2016-14:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.71.65.111	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.19.86.20	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
192.168.1.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
46.4.32.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
192.168.1.5		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.24.44	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
213.57.203.115	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
144.76.4.148	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.158	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-09-2016-13:04:08 to 03-09-2016-14:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
81.218.89.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.58.87	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.157.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.203.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.197.254.53	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
104.156.247.204	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
81.218.190.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.243.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.99	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.138.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
149.88.186.9	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.197.254.53	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
84.109.4.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-09-2016-13:04:08 to 03-09-2016-14:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
132.66.235.218	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	94
31.171.244.115	Switzerland	147.237.77.216	dover.idf.il	drop	SAM rule	drop	93
132.66.235.218	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	85
31.171.244.115	Switzerland	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	61
109.65.59.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
2.54.140.44	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	44
2.54.140.44	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
2.54.140.44	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	18
2.54.140.44	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
176.13.5.55	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
132.66.235.218	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.188	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.175	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
37.142.243.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
62.219.115.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.140.44	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
212.199.251.227	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
83.136.253.188	United Kingdom	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Anonymous DoSer Denial of Service Tool	reject	8
212.199.251.227	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
37.238.164.88	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.167	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
85.130.216.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.243.197	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
37.26.147.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.117.182.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.166.136.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.19.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.140.44	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack		reject	6
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.168.89.106	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
5.29.212.105	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
31.168.89.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.142.223.39	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.116.134.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.132	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
213.125.23.90	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.108.185.43	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.132	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.131	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence		monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.136.253.188	United Kingdom	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 83.136.253.188	Block	109
2.54.140.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
37.26.146.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
80.246.136.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
37.26.146.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
37.26.146.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
216.35.195.247	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	6
109.253.147.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.133.249	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.52.36.82	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	3
46.19.85.147	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
80.246.130.57	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
89.138.186.252	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/926-he/refuah.aspx	Block	2
62.28.244.1	Portugal	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	2
37.26.146.240	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
185.89.217.234		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.33	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtContent	Block	1
37.26.146.168	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.52.172.252	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/yassin2.wmv http:/opensky-media.com/de/arunachalashiva/excerpts.php	Block	1
80.178.98.149	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.89.217.226		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
62.219.234.126	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.172.225.223	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
2.54.153.175	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$4 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
198.175.126.98	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14160-he/dover.aspxהאוגדה	Block	1
185.112.248.32		147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
132.66.235.218	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.109.137.242	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
217.160.155.145	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
2.54.34.148	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1437-he/atal.aspx	Block	1
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
80.178.98.151	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.89.217.229		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/templates/sendtofriend/sendtofriend.aspx	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 38.111.147.88	Block	1
93.174.93.218	Netherlands	147.237.77.74	law.idf.il	NULL Character in Method	Block	1
5.29.212.105	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
208.115.113.89	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
73.129.92.126	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper	Block	1
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.185.250.106	Jordan	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
88.161.117.91	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.146.240	Israel	147.237.0.19	madim.atal.idf.il	Illegal Parameter Encoding ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/mobile/1088-he/meretz.aspx	None	1
2.54.34.148	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
193.105.199.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1