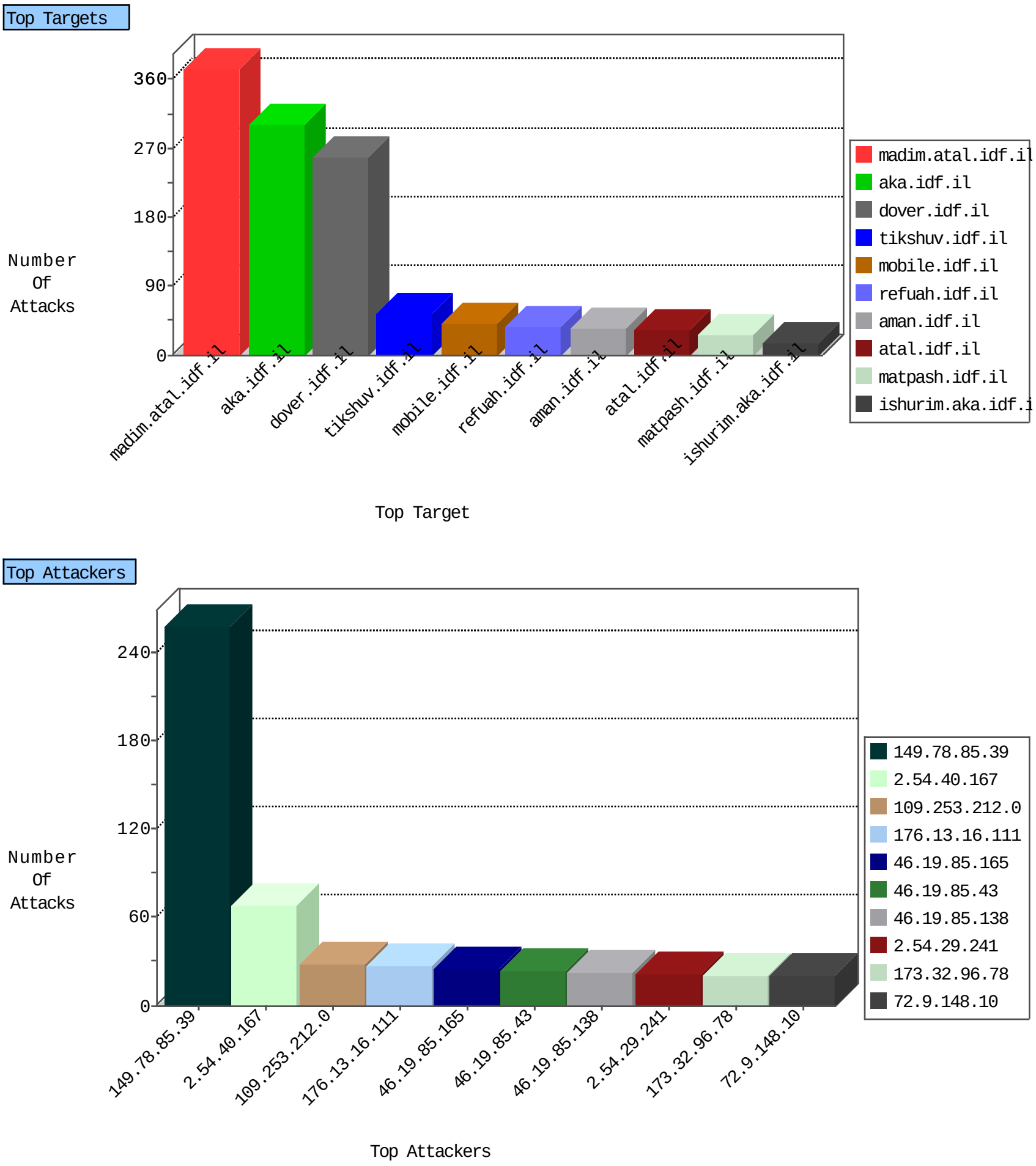
03-08-2016-17:04:03 to 03-08-2016-18:04:03

IDF Under Attack Daily Report



03-08-2016-17:04:03 to 03-08-2016-18:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
71.6.165.200	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
23.228.114.2	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.41	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
23.228.114.2	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
71.6.33.147	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
188.138.102.50	Germany	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1

03-08-2016-17:04:03 to 03-08-2016-18:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.197.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
46.117.45.188	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	7
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	7
5.29.26.41	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
5.28.174.114	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
2.52.162.34	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.120.53.37	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
46.19.85.49	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-08-2016-17:04:03 to 03-08-2016-18:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.29.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.89.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.234.8	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.192.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
66.102.8.250	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
194.90.244.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.139.27.231	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
192.117.127.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.139.27.231	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.221	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.66.56.84	147.237.77.216	Italy	dover.idf.il	portscan: TCP Distributed Portscan	1
37.1.209.203	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
109.67.191.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
88.247.137.156	147.237.8.45	Turkey	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.181.237.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.151.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.170.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
207.232.27.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.40.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.118.11.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.139.27.231	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
192.114.23.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.60.42.104	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.3.147.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.1.209.203	147.237.72.217	United States	e.idf.il	ET SCAN Potential SSH Scan	1
109.253.194.124	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-08-2016-17:04:03 to 03-08-2016-18:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.16.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
173.32.96.78	Canada	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
217.35.100.40	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
46.19.85.138	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
37.26.146.206	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.166.212.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.179.228.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.8.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.168.225.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.2	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.113	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.210.184.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
77.127.163.149	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.44.136	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.52.37.59	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
87.71.90.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.200	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
212.179.226.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.144.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.109.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.240.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.188	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.16.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.138	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.29.241	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.24.207.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
82.102.169.113	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
66.102.8.137	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
37.48.53.98	Czech Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.22.131.85	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.29.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
66.102.9.68	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
79.179.110.63	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.29.241	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.232	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
188.120.148.153	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.29.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

03-08-2016-17:04:03 to 03-08-2016-18:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.85.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	258
2.54.40.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
109.253.212.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
46.19.86.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.0.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.226.186	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	3
84.108.235.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.16.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
86.106.18.51	Romania	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
5.22.131.85	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	3
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.179.21.194	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/images/1.he/infocenteritem/	Block	1
79.181.109.239	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
188.43.123.70	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
37.26.146.240	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
137.226.113.7	Germany	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on 147.237.76.147/	Block	1
80.246.130.176	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.176	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
192.198.151.43	Europe	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/haredim/scriptresource.axd	None	1
46.19.85.94	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
89.139.237.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/personaldetails	Block	1
79.181.210.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.181.210.106	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
188.43.123.70	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1398-en/dover.aspx	Block	1
37.26.148.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
141.212.122.209	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
197.163.92.151	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.69.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/8/106938.pdf	Block	1
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 46.19.85.232	Block	1
2.54.149.71	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.181.210.106	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
66.249.64.153	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/news/news.in.aspx	Block	1
188.43.123.70	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1398-en/dover.aspx	Block	1
38.98.125.162	United States	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
197.163.92.151	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
185.82.200.91		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.232	Block	1
79.181.231.203	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
190.229.126.84	Argentina	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.2.163	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
40.77.167.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
87.69.62.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
207.46.13.87	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chinuch/miktzoa/default.asp	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	1
185.112.248.32		147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.232	Block	1
31.13.112.117	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/&h=uaqhyd1x0&enc=azmniafhix46vm4yxyrdikucev99ae3lsosjivbqybpinrlepiovaxfgebbkkzvt87yfmfzeqmrg4lnyaazbxzqb7pc0lv4jukeff0pnvtif9xfdbywtixzmqymqnk1_e0jzzxdj8hpozqvvcrthkvbzzr5ne6l1zcem4h3bhf0e9eqv--tzlioo16sqfb40ic&s=1لبنكا	Block	1
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

03-08-2016-17:04:03 to 03-08-2016-18:04:03