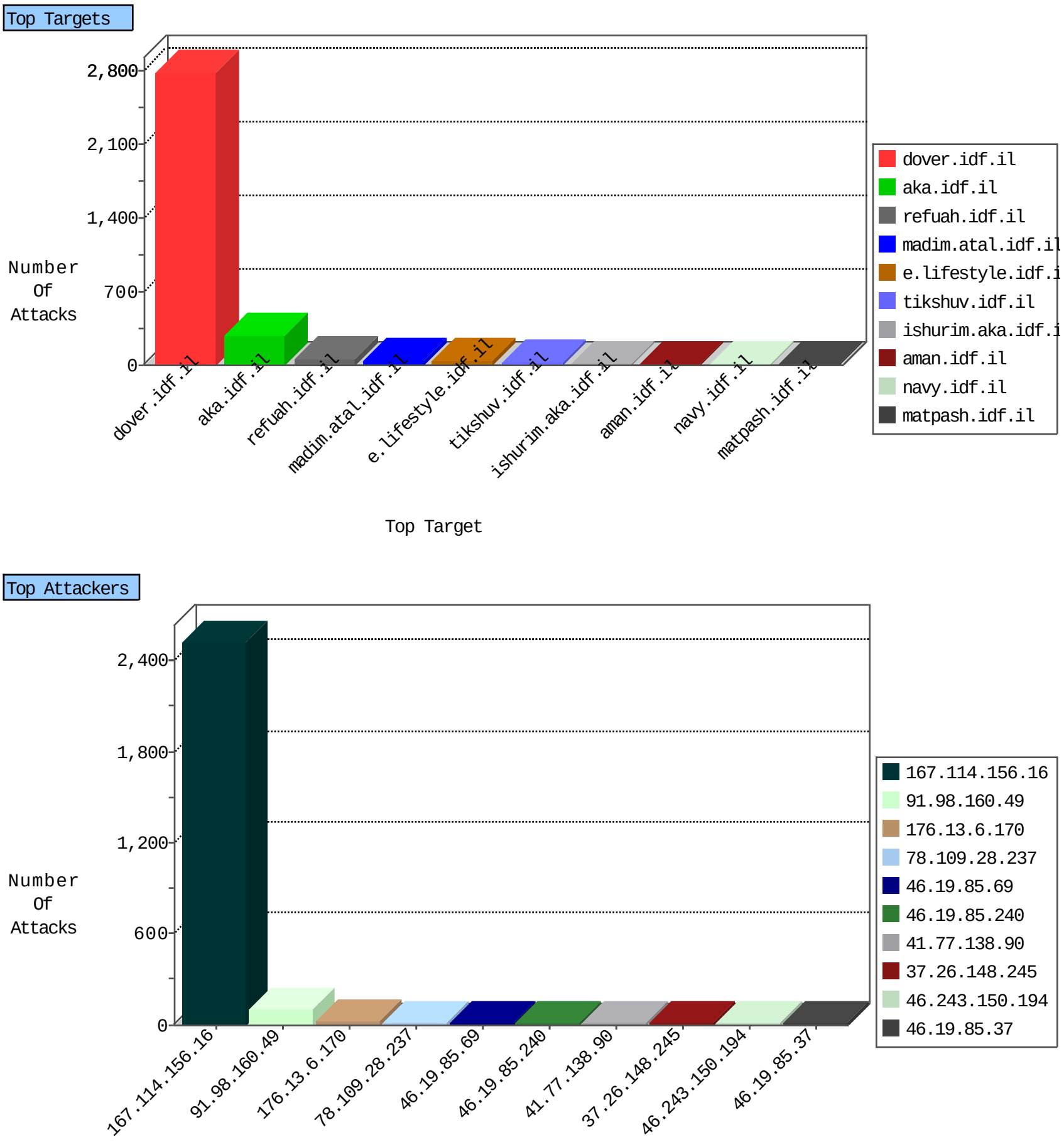
03-15-2016-14:04:04 to 03-15-2016-15:04:04

IDF Under Attack Daily Report



03-15-2016-14:04:04 to 03-15-2016-15:04:04

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	3625
91.98.160.49	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	385
146.185.57.8	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
146.185.57.8	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
82.145.223.137	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	2
213.52.178.166	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
213.52.178.162	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
213.52.178.163	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
182.140.167.188	China	147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
213.52.178.164	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
212.143.254.66	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

03-15-2016-14:04:04 to 03-15-2016-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.201.89	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
79.180.135.225	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
79.180.193.215	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
195.154.185.20	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	1
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	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-15-2016-14:04:04 to 03-15-2016-15:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.98.160.49	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN NMAP -sS window 1024	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
193.105.134.220	147.237.72.166	Sweden	aka.idf.il	ET SCAN NMAP -sS window 1024	1
45.35.64.142	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.138.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.143.82.50	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 2048	1
95.35.4.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.135.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.71.14.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.178.134.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.216.84.147	147.237.76.176	Taiwan	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
46.117.246.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.241.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.63.0.76	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.144.248	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.143.82.50	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 4096	1
109.65.71.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.143.82.50	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -f -sS	1
93.94.40.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.36.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.216.119.94	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.220.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
61.216.84.147	147.237.76.202	Taiwan	e.halag.idf.il	ET SCAN Potential SSH Scan	1
46.121.71.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-15-2016-14:04:04 to 03-15-2016-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	79
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	26
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	26
78.109.28.237	Ukraine	147.237.8.24	e.lifestyle.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	18
41.77.138.90	Egypt	147.237.8.24	e.lifestyle.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	15
46.243.150.194	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.19.85.37	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.154.251.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.17.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.165.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.240	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.52.26.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.148.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
81.218.198.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
2.54.145.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
84.108.168.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.120.142.97	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
82.80.141.195	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
109.65.64.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.110.48.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.22.135.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.109.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.240	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.219.163.115	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
192.114.23.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
107.6.123.226	Singapore	147.237.8.24	e.lifestyle.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	4
37.26.148.233	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	4
62.219.163.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.67.140.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.130.158	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.168.217.255	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.194.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.66.80.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.160.242.40	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.146.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
80.179.207.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.40.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.176.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.195.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.238.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.6.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
185.120.126.4		147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 185.120.126.4	Block	10
46.19.86.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
176.13.20.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.226.44.156	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
176.13.22.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.213.161.17	Romania	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
207.46.13.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.179.13.141	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 80.179.13.141	Block	2
41.36.125.132	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.52.165.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.233	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
70.39.157.194	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
31.154.25.158	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
109.226.22.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.17.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.168.13.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
197.164.177.141	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.146.137	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.52.132.102	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.23	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
41.68.161.204	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
109.64.188.204	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
84.111.24.80	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 84.111.24.80 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
37.26.148.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1397-en/dover.aspx	Block	1
68.180.230.43	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/1104-he/eitan.aspx	None	1
31.154.25.158	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 31.154.25.158	Block	1
192.114.177.190	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	1
167.220.196.186	United Kingdom	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.120.142.97	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
87.71.56.43	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
37.26.146.149	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
207.46.13.160	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
81.218.251.250	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/70902.pdf	Block	1
185.32.179.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.226.17.214	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.111.24.80	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1438-he/dover.aspx	Block	1
197.38.175.202	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
54.191.216.77	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
87.169.119.169	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/an	Block	1
41.47.102.234	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
37.26.146.179	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.171	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
82.80.141.195	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/key/aswd56425csa	Block	1