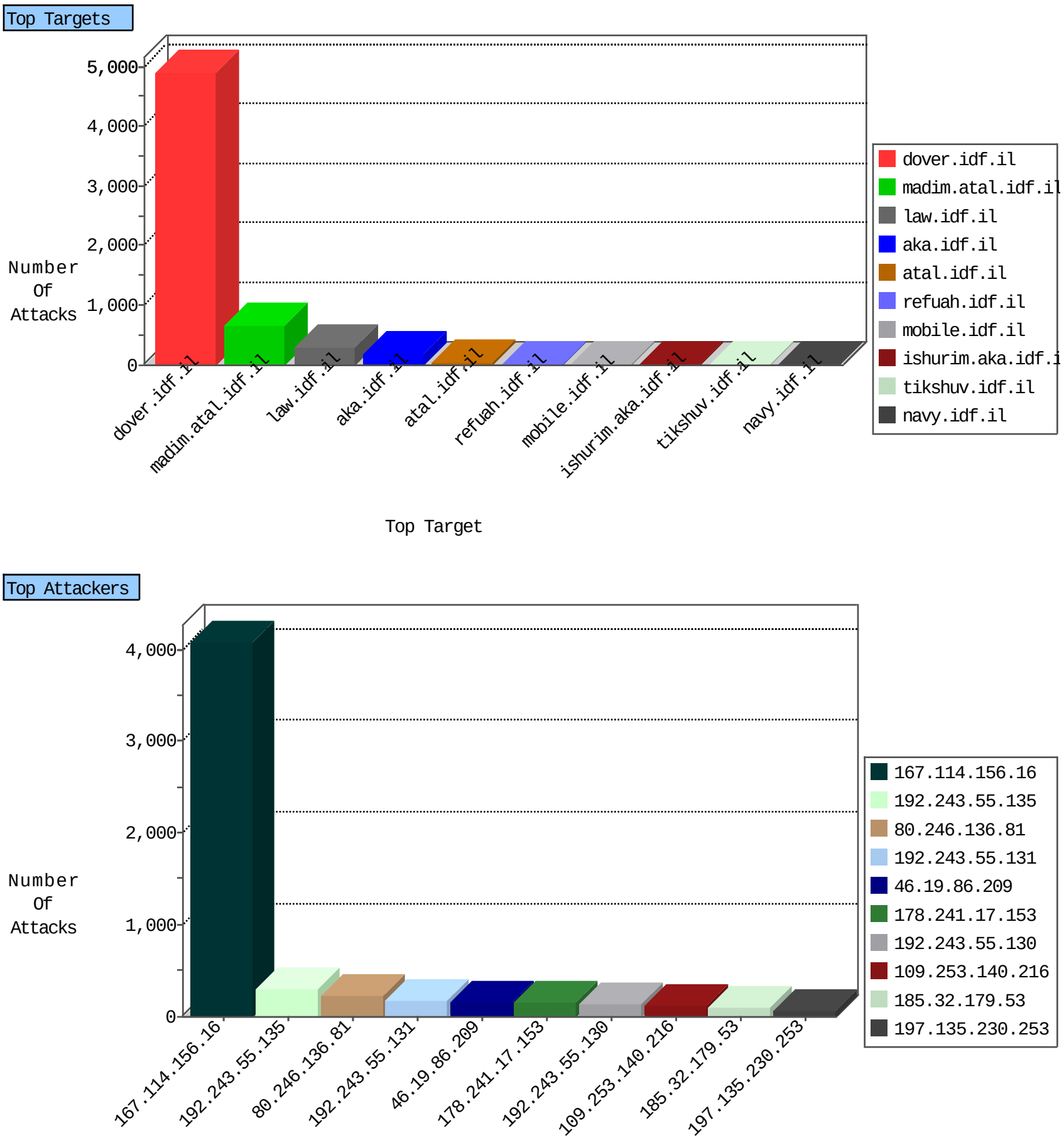
04-12-2016-19:04:04 to 04-12-2016-20:04:04

IDF Under Attack Daily Report



04-12-2016-19:04:04 to 04-12-2016-20:04:04

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	Block_Ip_Web_In	drop	4077
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	450
81.218.125.182	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	97
79.180.162.189	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	50
41.107.2.205	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	33
80.246.133.72	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
85.250.187.117	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
192.243.55.135	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
31.168.240.21	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
82.145.223.56	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	3
84.228.223.225	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
197.135.230.253	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
31.210.188.49	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
109.67.142.234	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
91.126.252.47	Spain	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
77.125.142.103	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
94.102.49.116	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
176.31.60.249	France	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
66.240.236.119	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
176.31.60.249	France	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
217.112.96.194	Italy	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

04-12-2016-19:04:04 to 04-12-2016-20:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.7.56	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.85.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.86.8	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	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
61.135.189.122	China	147.237.76.31	nakchal.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
71.6.146.185	United States	147.237.76.38	e.e.meitav.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-12-2016-19:04:04 to 04-12-2016-20:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.74	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	14
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.93.79	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	4
77.125.84.30	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
185.32.179.53	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
79.177.183.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.103	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
185.125.216.75	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.103	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
184.151.114.104	147.237.72.166	Canada	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.103	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
88.204.187.90	147.237.0.19	Kazakstan	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
88.204.187.90	147.237.0.19	Kazakstan	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
80.246.136.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.142.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.76.34	United States	yohalan.idf.il	ET DROP Dshield Block Listed Source	1
192.243.55.135	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.103	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	147.237.0.200	Turkey	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
5.22.135.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
88.204.187.90	147.237.0.19	Kazakstan	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
87.69.20.217	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

04-12-2016-19:04:04 to 04-12-2016-20:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
178.241.17.153	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	96
197.135.230.253	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	46
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	37
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
192.243.55.135	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	32
192.243.55.131	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	30
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	28
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	28
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	22
192.243.55.131	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
192.243.55.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
178.241.17.153	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
178.241.17.153	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.131	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	14
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
109.64.37.191	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
178.241.17.153	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
207.46.13.74	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	12
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	11
192.243.55.130	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.131	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	11
81.218.125.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
149.78.192.195	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
178.241.17.153	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	10
46.19.85.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.130	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.200	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.38.147.7	Hungary	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
5.102.254.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	233
46.19.86.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	163
109.253.140.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	127
185.32.179.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	105
5.189.190.212	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
37.26.149.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
174.129.237.157	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 174.129.237.157	Block	3
109.253.139.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.212.142	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
80.246.137.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
66.249.66.186	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.122	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.54	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.143.30	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
110.138.44.30	Indonesia	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
64.79.85.205	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/shared/usercontrols/headerupper/	Block	1
217.132.151.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.138	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/...	Block	1
95.213.6.27	Russian Federation	147.237.76.31	nakchal.idf.il	URL is Above Root Directory www.nakhal.idf.il/1115-he/../../images/shared/mailthisclose.png	Block	1
185.32.179.165	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
5.39.222.159	Netherlands	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
110.138.44.30	Indonesia	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
84.228.226.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	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
37.187.114.171	France	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to /irj/portal	Block	1
79.182.212.210	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
192.243.55.135	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0121-	Block	1
5.39.222.159	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
131.253.25.196	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.65.154.137	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
174.129.237.157	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/forums.frm/frmprintmessage.aspx	Block	1
37.187.114.171	France	147.237.77.74	law.idf.il	Unauthorized URL Access to /irj/portal	Block	1
80.178.102.199	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.120.20.241	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
5.189.18.170	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
87.71.2.72	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
66.249.66.186	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
185.17.232.83	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
41.107.2.205	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1451-11993-he/dover.aspx'	Block	1
54.153.33.145	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
207.46.13.161	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
157.55.39.65	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
89.247.67.37	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
68.194.87.109	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
46.19.85.161	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1