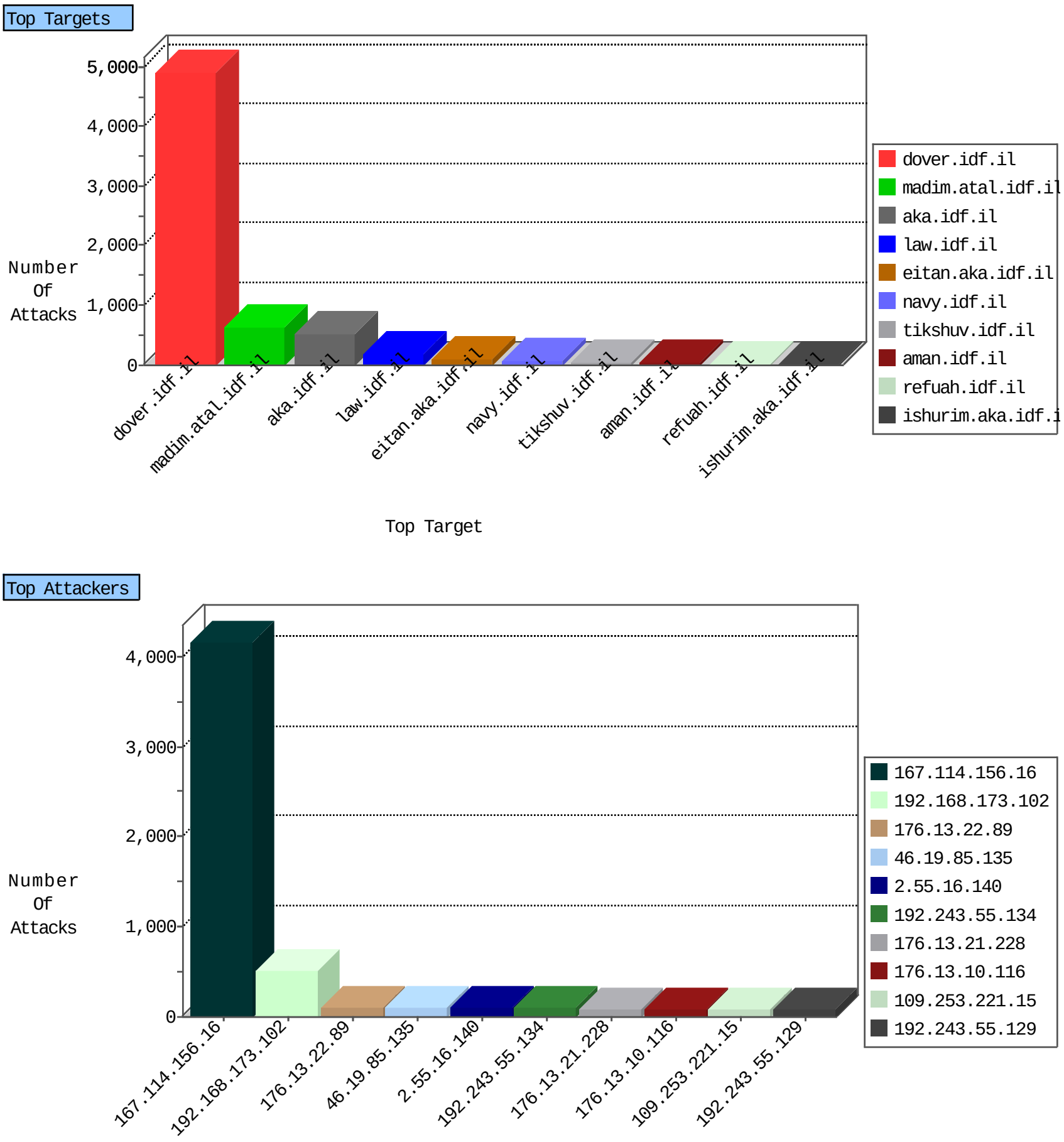
04-11-2016-08:04:00 to 04-11-2016-09:04:00

IDF Under Attack Daily Report



04-11-2016-08:04:00 to 04-11-2016-09:04:00

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	4173
192.243.55.131	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	295
192.243.55.135	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	276
62.219.140.244	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	134
192.243.55.136	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	121
185.46.212.74	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	30
185.32.179.106	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
120.132.50.135	China	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	4
168.235.197.216	United States	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
168.235.197.216	United States	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
147.236.232.254	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.243.55.134	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
109.253.206.6	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
164.138.23.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
179.43.144.50	Switzerland	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
79.180.167.112	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
179.43.144.50	Switzerland	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
139.190.41.7	Pakistan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
10.33.254.3		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
80.246.133.225	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.243.55.137	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.247.239	United States	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1

04-11-2016-08:04:00 to 04-11-2016-09:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.14.26	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
109.253.134.127	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
88.198.230.79	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
88.198.230.79	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
109.253.145.79	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
88.198.230.79	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
176.13.11.20	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	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	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-11-2016-08:04:00 to 04-11-2016-09:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
175.43.95.77	147.237.77.216	China	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	2
213.8.242.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.76.44	United States	e.refuah.idf.i	ET SCAN NMAP -sS window 1024	1
192.243.55.130	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
168.235.197.216	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
104.232.98.3	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
87.69.127.238	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.253	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
52.16.5.197	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
217.69.133.190	147.237.72.166	Russian Federation	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.205.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
107.196.28.141	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
87.70.91.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.14.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.131.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.255	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-11-2016-08:04:00 to 04-11-2016-09:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	344
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	168
207.232.27.5	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
168.235.197.216	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	55
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
192.243.55.129	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
192.243.55.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.129	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
62.219.140.244	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
37.26.147.245	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.218.53	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.128.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.138	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.132	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
72.181.132.230	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.129	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.134	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.135	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.134	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.134	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
85.130.216.49	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
80.246.139.24	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
172.89.89.209	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.134	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.134	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.131	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
85.130.216.49	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.226	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.135	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.129	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
85.65.220.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.135	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

04-11-2016-08:04:00 to 04-11-2016-09:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.22.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
46.19.85.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	108
2.55.16.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	93
176.13.21.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	91
176.13.10.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	88
109.253.221.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	85
176.13.20.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
192.114.23.18	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 192.114.23.18	Block	13
2.54.164.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	6
37.142.64.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
80.246.137.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
185.32.179.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
185.32.179.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.5.140	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.133.225	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.54.189.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	3
131.253.25.164	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.180.233.225	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	2
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	2
68.180.231.43	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.231.43	Block	2
176.13.14.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
175.43.95.77	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 175.43.95.77	Block	2
66.249.78.22	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
175.43.95.77	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-9703-en/dover.aspxjavascript:window.open(http:/www.gadnaot-navy.co.il,,toolbar=true,menubar=true,truescrollbars=trueresizable=true)	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	1
77.75.79.17	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/34/	Block	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1275-he/atal.aspx	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
175.43.95.77	China	147.237.72.166	aka.idf.il	Unknown Parameter amp in www.aka.idf.il/main/sachar/scriptresource.axd	None	1
85.65.220.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.243.55.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/nahal.stm.	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.86.69	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
199.203.136.177	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 199.203.136.177	Block	1
157.55.39.9	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
192.243.55.133	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
66.249.64.253	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.117	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
175.43.95.77	China	147.237.72.166	aka.idf.il	Unknown Parameter amp in www.aka.idf.il/main/sachar/webresource.axd	None	1
109.64.24.224	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
192.243.55.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59391&docid=65516	Block	1
192.114.23.18	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1806.jpg	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.86.78	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
207.232.5.252	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
175.43.95.77	China	147.237.72.166	aka.idf.il	Unknown Parameter amp in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1

04-11-2016-08:04:00 to 04-11-2016-09:04:00