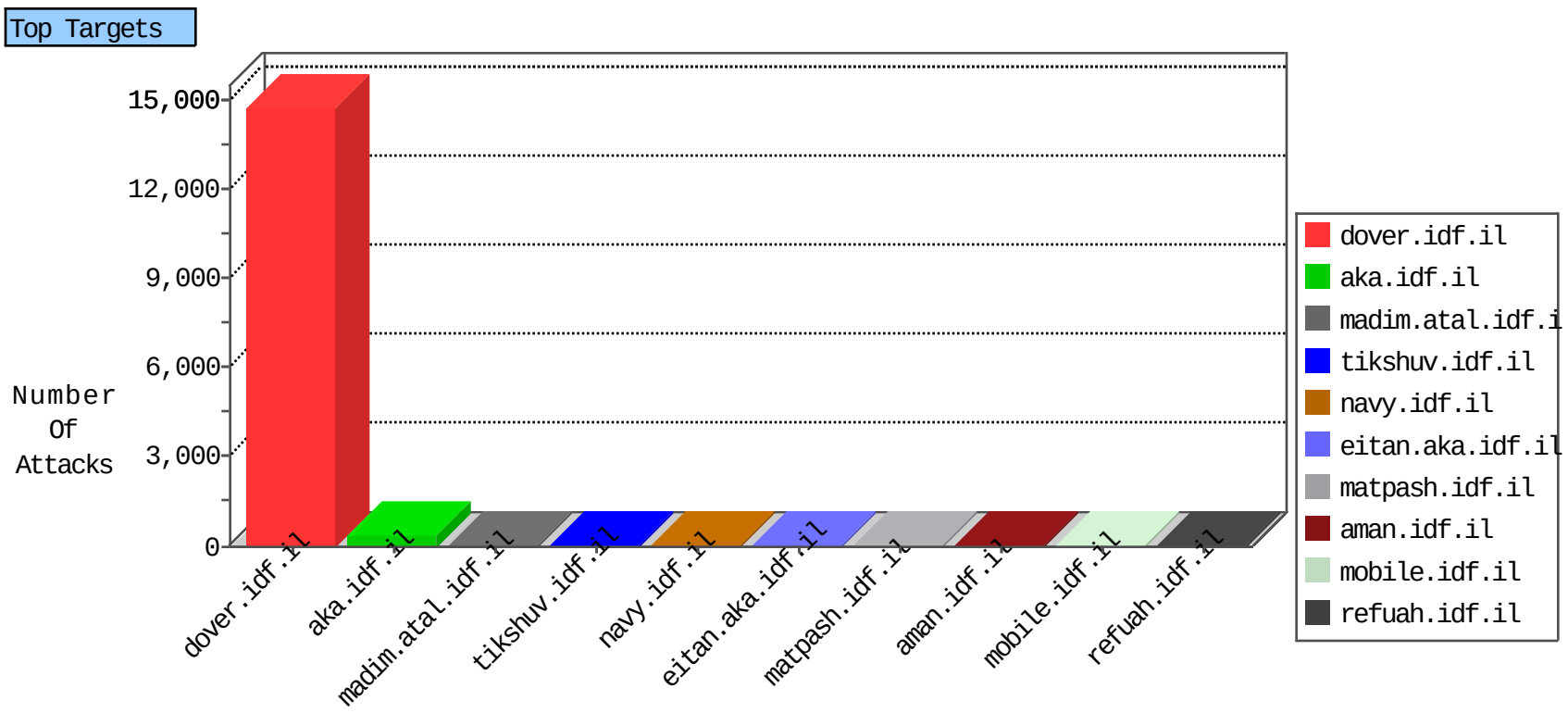
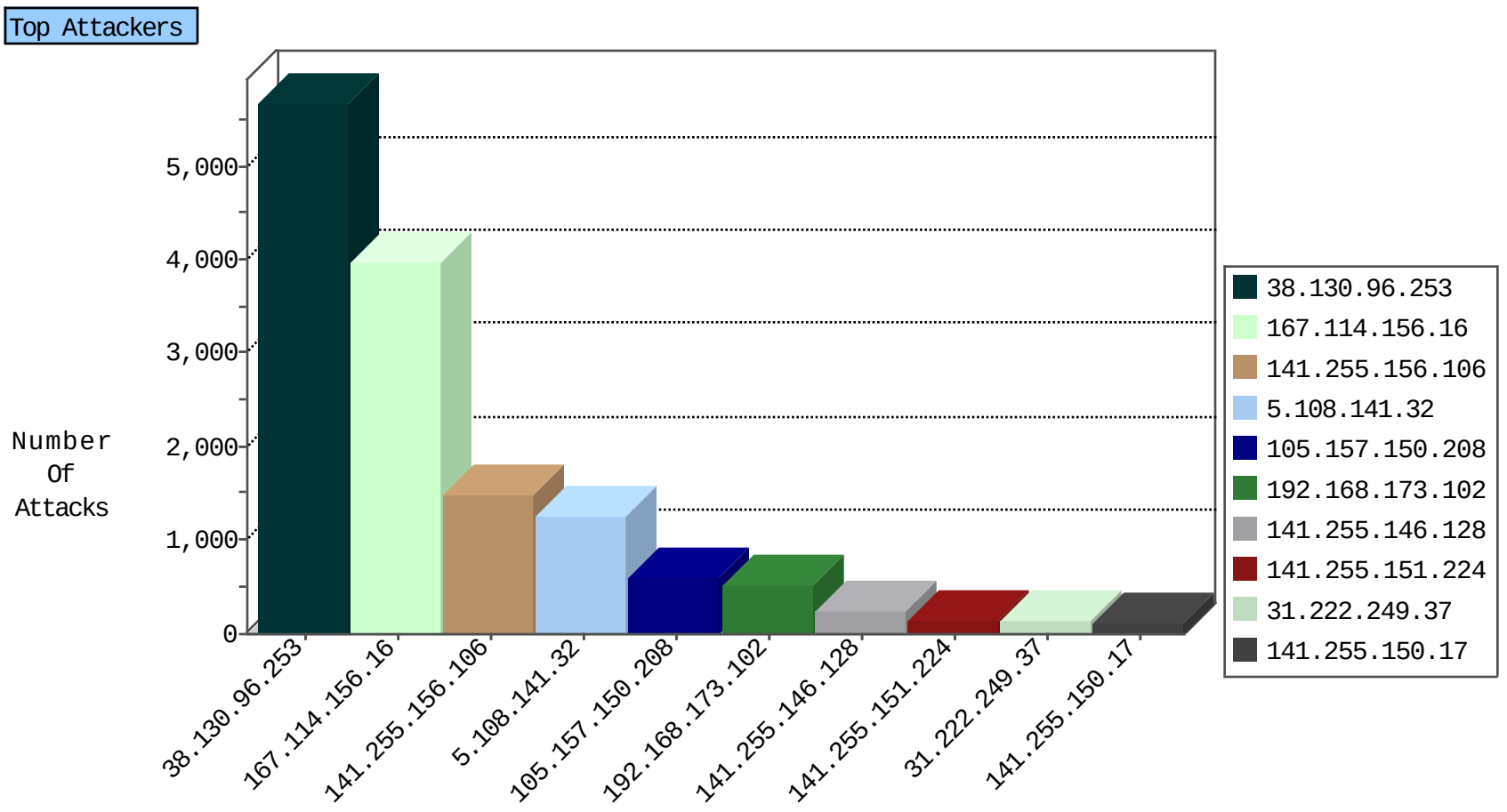
04-09-2016-22:04:03 to 04-09-2016-23:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-09-2016-22:04:03 to 04-09-2016-23:04:03

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	3970
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2230
38.130.96.253	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1556
38.130.96.253	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	960
141.255.156.106	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	427
38.130.96.253	United States	147.237.77.216	dover.idf.il	HTTP-MISC-DoS-GoodBye-30	dest-reset	335
46.121.96.110	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	237
141.255.146.128	Netherlands	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	230
141.255.156.106	Netherlands	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	147
141.255.151.224	Netherlands	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	146
31.222.249.37	Jordan	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	131
141.255.150.17	Netherlands	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	111
84.228.236.179	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	110
134.35.134.142	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	109
79.178.49.42	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	73
70.39.186.88	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	66
38.130.96.253	United States	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	57
37.26.148.216	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	20
38.130.96.253	United States	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	13
134.35.165.235	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
74.91.20.195	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
209.126.127.17	United States	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	2
173.208.197.251	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	2
69.197.185.20	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	2
107.150.46.36	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
69.197.185.22	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	2
107.150.32.59	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	2
107.150.32.60	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	forward	2
134.35.165.235	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
82.145.216.191	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1
209.126.127.17	United States	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
77.68.40.189	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.120.194.179	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
209.126.127.17	United States	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
185.56.28.67	Netherlands	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
209.126.127.17	United States	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
200.160.6.137	Brazil	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
209.126.127.17	United States	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

04-09-2016-22:04:03 to 04-09-2016-23:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.21.195	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	17
188.120.148.150	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.50.59.192	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	4
62.233.37.62	France	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	3
123.126.113.167	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
105.154.186.206	Morocco	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
104.167.254.30	Albania	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	2
2.53.3.145	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.i	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

04-09-2016-22:04:03 to 04-09-2016-23:04:03

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	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
122.3.71.72	147.237.8.50	Philippines	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.90.244.226	147.237.76.199	Germany	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
41.254.9.253	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	SERVER-WEBAPP admin.php access	1
85.90.246.134	147.237.76.198	Germany	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.0.15	Netherlands	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1

04-09-2016-22:04:03 to 04-09-2016-23:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
38.130.96.253	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2329
38.130.96.253	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	1530
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1245
141.255.156.106	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1081
105.157.150.208	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	460
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	346
38.130.96.253	United States	147.237.77.216	dover.idf.il	drop		drop	281
38.130.96.253	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	249
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	164
141.255.156.106	Netherlands	147.237.77.216	dover.idf.il	drop		drop	155
141.255.156.106	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	88
105.154.186.206	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	72
105.157.150.208	Morocco	147.237.77.216	dover.idf.il	drop		drop	68
77.68.40.189	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
105.157.150.208	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	50
70.39.186.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
37.26.149.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
38.130.96.253	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	37
105.104.42.205	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
38.130.96.253	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	23
46.19.85.150	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
176.13.0.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.67.228.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
80.246.139.160	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
37.26.149.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
84.228.236.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
105.157.150.208	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.182.60.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.139.160	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
95.86.78.14	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.147.150	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
46.121.96.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
94.55.219.155	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.13.43	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.109.2.49	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
81.18.213.246	Poland	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
77.125.103.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.51	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.205.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.51	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.46.39.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
78.165.204.30	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
81.18.213.246	Poland	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

04-09-2016-22:04:03 to 04-09-2016-23:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	6
185.120.125.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
86.69.5.24	France	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	5
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 5.108.141.32	Block	3
109.67.8.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	2
79.178.151.253	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$txtSearch in www.idf.il/1133-he/dover.aspx	Block	2
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
41.254.9.253	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
207.46.13.25	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
80.230.216.169	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
173.208.197.251	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to www.tt985.com/	Block	1
69.197.185.22	United States	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on www.tt782.com/	Block	1
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
105.157.150.208	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
80.230.216.227	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.178.165.157	Israel	147.237.72.156	aman.idf.il	Illegal Parameter Encoding catId in www.aman.idf.il/modiin/kiosk.aspx	None	1
196.218.59.224	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
109.253.205.112	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17032-he/dover.aspx	Block	1
87.71.18.251	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
41.254.9.253	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 41.254.9.253	Block	1
208.90.57.196	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
80.230.216.170	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
180.76.15.143	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/scroller/jquery.jcarousel.css	Block	1
74.91.20.195	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.tt782.com/	Block	1
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
107.150.32.59	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.tt782.com/	Block	1
80.230.216.228	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
38.130.96.253	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
79.178.165.157	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Parameter Encoding from 79.178.165.157	None	1
197.0.27.188	Tunisia	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
149.88.83.225	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/main/home/default.aspx	Block	1
93.172.162.142	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
41.254.9.253	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.254.9.253	Block	1
217.69.133.244	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/faq/default.asp	Block	1
80.230.216.171	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.75.78.165	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/33/	Block	1
180.76.15.149	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
109.64.239.180	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
84.110.36.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
41.109.2.49	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
80.230.216.68	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
197.0.27.188	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
156.203.4.82	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.93.68	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
41.254.9.253	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin	Block	1
105.154.186.206	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
80.230.216.172	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

04-09-2016-22:04:03 to 04-09-2016-23:04:03