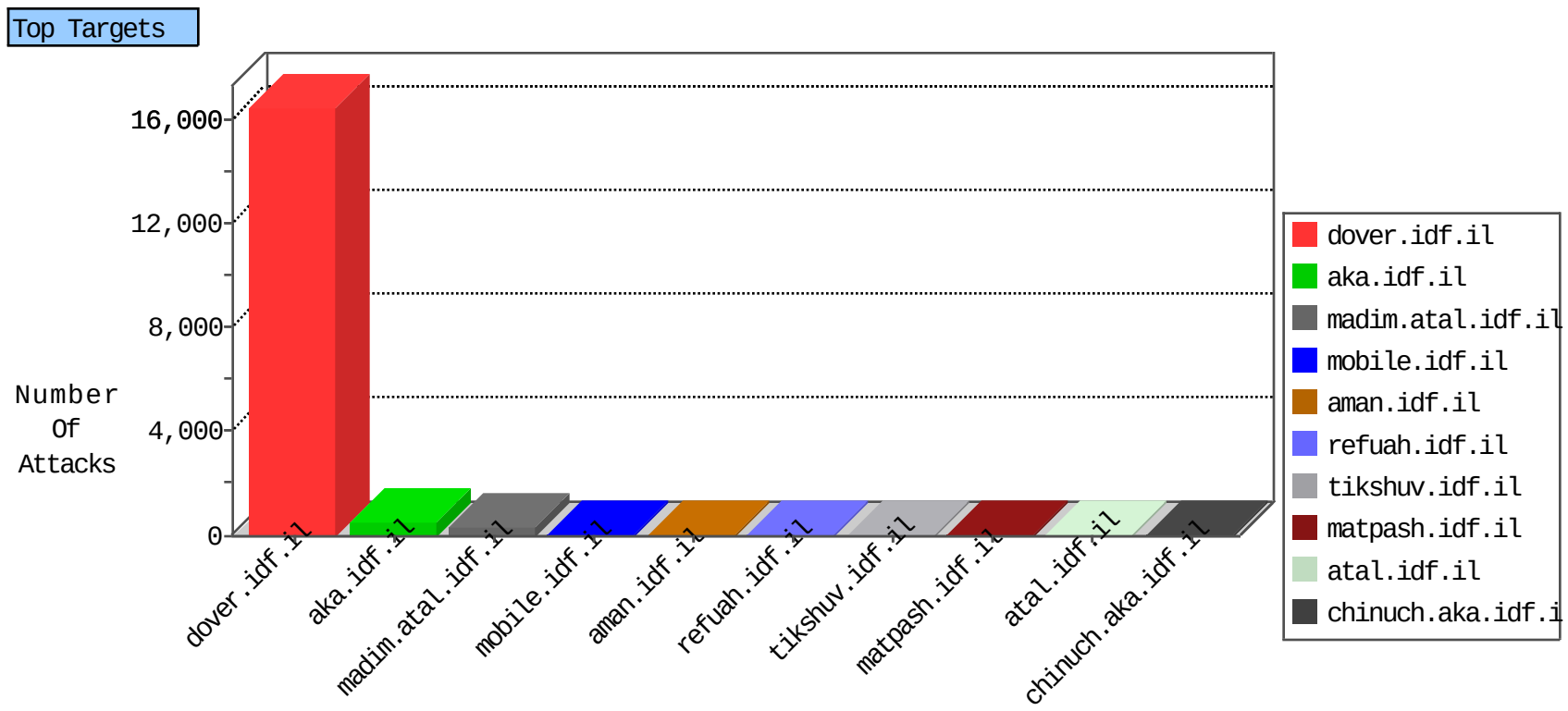
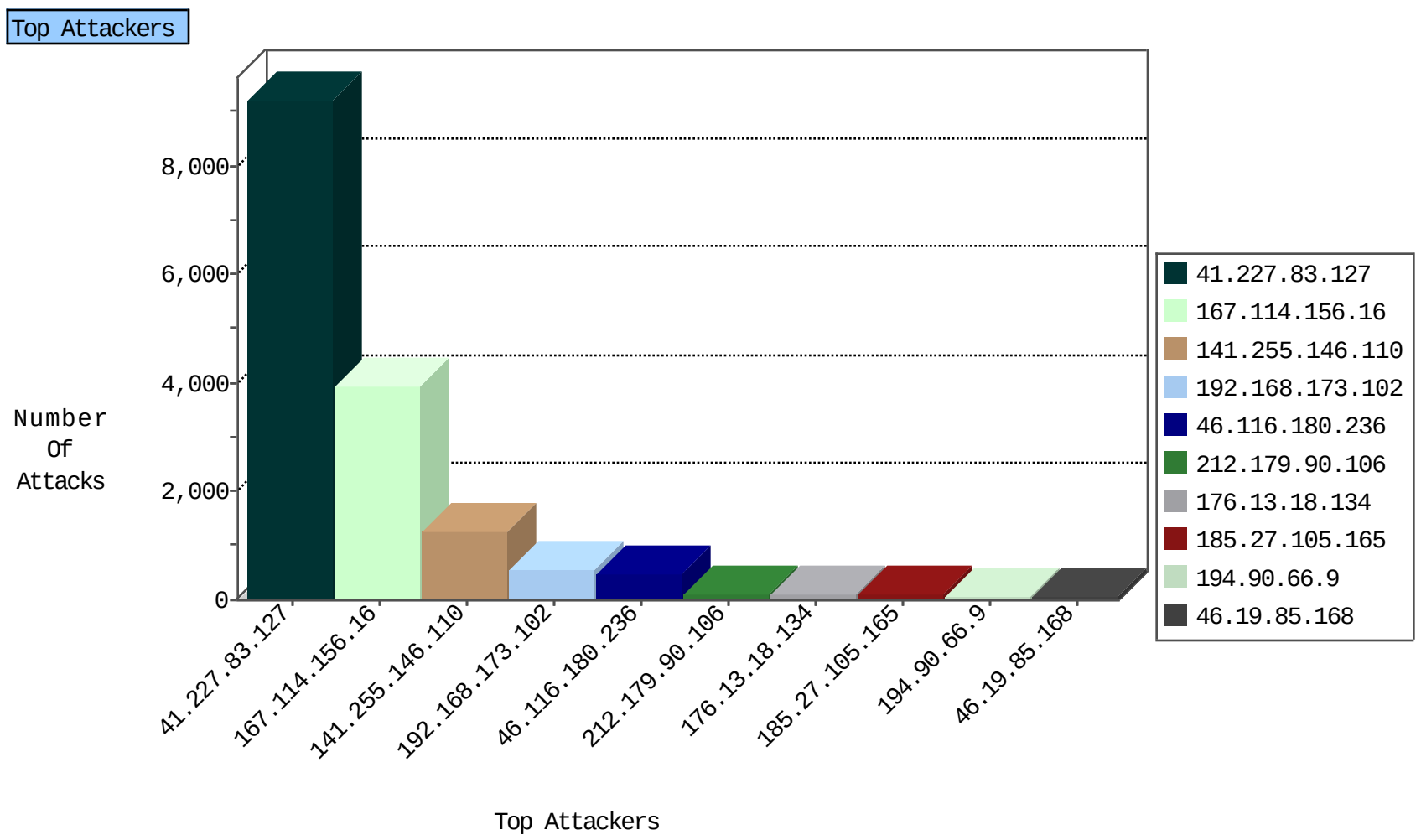
04-10-2016-16:04:01 to 04-10-2016-17:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-10-2016-16:04:01 to 04-10-2016-17:04:01

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	3916
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1126
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	741
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	546
141.255.146.110	Netherlands	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	442
192.249.66.247	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	285
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	175
192.115.98.205	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	50
41.227.236.35	Tunisia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	46
87.71.99.59	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34
212.76.127.10	Israel	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	21
212.76.127.219	Israel	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	18
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
46.116.180.236	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
69.30.202.226	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
204.12.196.236	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
46.19.85.84	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
69.30.226.99	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	2
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
79.181.150.127	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
74.91.17.179	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	2
31.154.4.36	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
36.70.194.1	Indonesia	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
141.255.146.110	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
77.126.51.114	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
41.137.59.31	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
23.222.28.185	Netherlands	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
46.19.85.214	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
198.62.219.8	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
108.166.11.20	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
192.114.91.246	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
199.203.100.145	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
77.125.5.154	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-10-2016-16:04:01 to 04-10-2016-17:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.10.204	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
212.76.101.25	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.179.249.80	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
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
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-10-2016-16:04:01 to 04-10-2016-17:04:01

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
193.106.52.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.86.64.27	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.110.36.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.125.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.182	147.237.72.166	Europe	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.218.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.252.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.65.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
202.152.10.104	147.237.0.34	Indonesia	tikshuv.idf.i	ET SCAN Potential SSH Scan	1
104.245.235.99	147.237.76.196	United States	e.sviva.idf.i	ET SCAN NMAP -sS window 1024	1
89.138.190.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.166.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.163.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.61.38	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.64.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.41.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.130.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.25.105.125	147.237.72.156	Israel	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
199.203.226.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-10-2016-16:04:01 to 04-10-2016-17:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8014
141.255.146.110	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	809
46.116.180.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	469
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	371
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	drop		drop	239
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	168
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	116
185.27.105.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	87
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
85.64.194.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
37.26.149.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
212.76.127.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
105.101.29.158	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
212.76.127.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
141.255.146.110	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
199.115.117.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.118.11.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.53.28.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
169.1.17.177	South Africa	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.8.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.234	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
153.25.178.60	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.3.147.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.54.143.255	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
37.26.147.224	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
37.26.148.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.183	Israel	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	9
109.67.63.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
31.210.187.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
176.0.63.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
104.131.178.69	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.179.42.242	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
82.166.184.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.58	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
84.95.2.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7

04-10-2016-16:04:01 to 04-10-2016-17:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
194.90.66.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
46.19.85.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
176.13.10.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
176.13.18.191	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
109.253.202.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.13.4.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.149.234	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
85.250.61.29	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	5
2.54.135.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
217.132.38.117	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 217.132.38.117	Block	3
37.26.148.146	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	2
80.246.136.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
46.19.85.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.29.23	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.18.134	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	2
5.10.229.226	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/ط	Block	2
46.19.85.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.7.200	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
199.115.117.194	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/dover.aspx'	Block	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version Þ“k„wp^”žŽÿþØõ¿ž'•[[#1]]÷•~Ûæ¢CüÒåÁJ[[#30]]ËF[[#23]]À[[#22]]ÿ^•]œ”€G—°Žì[[#25]]Îý[[#11]]ó—[[#0]]ŽmÝýßÂÚ•»•À‚ë«[[#15]]¯®Ü[[#22]]<‰•Æ[[#4]]Ãƒ)†[[#28]]_n_Û[[#16]]ØsÌ[[#0]]Ò??	Block	1
74.82.47.2	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
176.13.17.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.121.232.50	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 103 cookies	Block	1
114.97.56.215	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1328-he/cogat.aspx/trackback/	Block	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method ±³Qm”V•Î&…[[#15]]þçÔÆ(¢ˆ¹[[#29]]w³•cU’EN in URL ’¸¤ [[#1]]5m[[#16]]+<û¿9|'%gixr]‹¡	Block	1
213.8.204.50	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
185.120.125.9	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
169.229.3.90	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/rec.dat	Block	1
204.12.196.236	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on www.369bs.com/	Block	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding ’[[¸¤#1]]59¿û<+]]61#[[m|¡‹]rxig%'	Block	1
74.91.17.179	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
141.212.122.129	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to /x	Block	1
79.183.59.235	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.149.168	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Value	Block	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name ¡[[#19]][[#19]][[#21]]L?ÞËôU@¡ˆ[[#26]]»eÎÈËã´š'ØU[[#23]]¸^@[[#27]]®¤[[#27]]©[[#25]]î[[#1]]•àoè~•[[#24]]‡ÊL˜hV;d•[[#5]]£IO/åú±NE`·ËTÏä[[#6]]ö4™[[#18]]ç_ÓV+t?!—©Y@[[#6]]Ë¿xO‡%¾úñ…{Z’¶MãP[[#30]][[#12]][[#7]]G€–hgÜ[[#11]][[#24]][[#31]]Ü&-[[#21]]•[[#2]]&Î–Ù$j?¯#011[[#1]]ì¡V#mšæhbÕ,?\ÿ%¯šq—e[[#29]]Ÿuzó‰áS-•é$>¡;c,S$ðòË[[#17]]¶'þáK³XÙDFØhT±[[#21]]?[[#4]]Ž›òQJ[[#8]]Sàµl£X«ÏÐ[[#0]]ÀÑé(J[[#30]]'Ž%Ä[[#5]],N%põ[[#19]]¼[[#3]]å[[#12]] áá´"âÌ\Æ7Ø‰¢[[#15]]SµK«•vQÌ°®Sú,j	Block	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.164	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.25	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
79.180.66.117	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 5	Block	1
79.178.62.14	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.234	Block	1
141.255.146.110	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
79.183.201.192	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/default.aspx	Block	1
217.132.38.117	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
194.90.66.9	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtFirstName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1

04-10-2016-16:04:01 to 04-10-2016-17:04:01