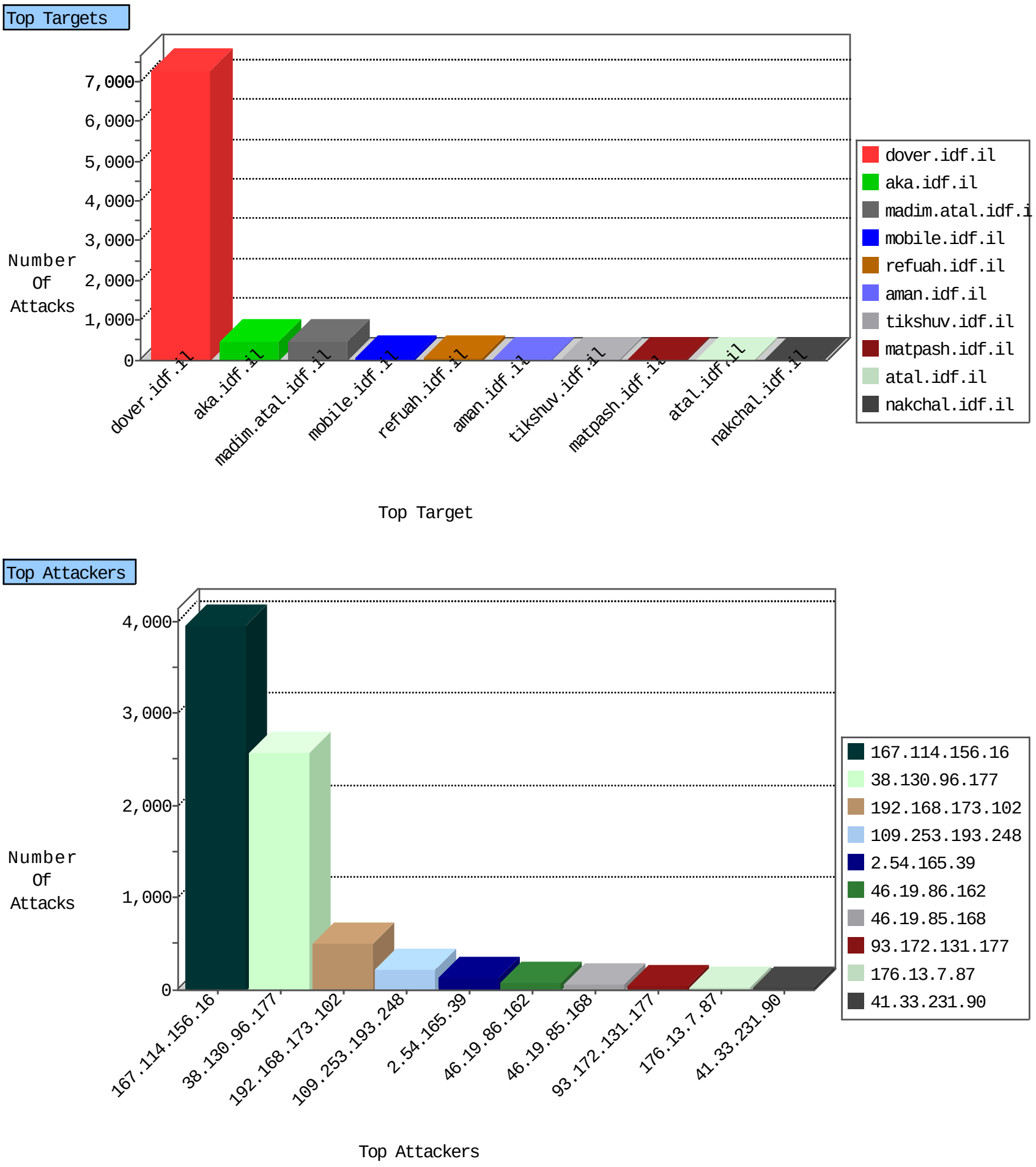
04-10-2016-18:04:09 to 04-10-2016-19:04:09

IDF Under Attack Daily Report



04-10-2016-18:04:09 to 04-10-2016-19:04:09

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	3965
38.130.96.177	United States	147.237.77.216	dover.idf.il	HTTP-MISC-DoS-GoodBye-30	dest-reset	2366
2.54.128.118	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1214
38.130.96.177	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	78
38.130.96.177	United States	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	58
38.130.96.177	United States	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	10
123.59.59.52	China	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	4
192.115.90.26	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
173.252.95.23	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
93.233.4.241	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
185.94.111.1	Russian Federation	147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
46.19.86.97	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
41.100.138.154	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.244.90.31	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.85.20	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
176.31.60.249	France	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
46.19.86.47	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
2.54.137.201	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-10-2016-18:04:09 to 04-10-2016-19:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.71.66.97	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
87.69.89.8	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.120.162.57	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
185.120.125.25	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
106.185.37.254	Japan	147.237.77.233	atal.idf.il	C1000016: HTTP: administrator in URI	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-10-2016-18:04:09 to 04-10-2016-19:04:09

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	3
173.88.225.181	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
173.88.225.181	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
88.204.187.90	147.237.0.16	Kazakstan	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.96.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.210.239.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.241.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
1.34.5.124	147.237.0.15	Taiwan	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
189.218.249.49	147.237.77.121	Mexico	e.navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
189.218.249.49	147.237.77.19	Mexico	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
173.88.225.181	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
89.248.162.167	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.108.32.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.96.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
219.135.123.117	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
40.84.149.32	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 3072	1
208.100.26.228	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.52.181	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
189.218.249.49	147.237.77.61	Mexico	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

04-10-2016-18:04:09 to 04-10-2016-19:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
38.130.96.177	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1359
38.130.96.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	518
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	330
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	174
46.19.86.162	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	85
93.172.131.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
192.171.234.22	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
109.253.221.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
73.253.227.193	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.182.186.178	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
93.172.7.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.53	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.65.111.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.183.96.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
87.70.7.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.147.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.186	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
46.19.85.193	Israel	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	8
2.52.129.178	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
89.138.170.37	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
213.57.243.91	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.103	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	7
87.70.104.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.160.191.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.133.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.109.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.168	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.248.69	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
2.54.131.9	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.157	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.138.75	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.244.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.248.69	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
37.26.147.157	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.54.130.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
85.64.32.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.160.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.168	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
172.58.168.37	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.64.74.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.102.254.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.193.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	216
2.54.165.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
46.19.85.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
176.13.7.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
2.54.130.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
131.253.25.220	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
37.26.148.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
95.86.127.73	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	5
109.253.221.205	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
109.253.197.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.193.248	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	3
212.34.23.72	Jordan	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 212.34.23.72	Block	3
2.55.55.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.34.23.72	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 212.34.23.72	Block	3
212.34.23.72	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.34.23.72	Block	3
46.51.199.64	Ireland	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.51.199.64	Block	3
199.30.24.154	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.34.23.72	Jordan	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 212.34.23.72	Block	2
199.30.24.168	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.12.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.138.75	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
199.30.25.52	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
213.57.226.203	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.53	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
199.30.25.119	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.183	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.34.23.72	Jordan	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 60302533.1.1460302557.1460302533.; in URL _pk_ses.20.8afc=*	Block	1
199.255.210.172	Anonymous Proxy	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	Block	1
96.233.178.243	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in URL d±[[#27]]"[[ך´¸‰½ק•#1ע]] u[[#16]]hŒi6z¡![[#4]]¨ו5[[¿•#23µž]]מט[[13#]]…Ùו-ג ´z[[#14]][[#8]]×‹[k^l•ü¨qף·Ê-qcˆ›pn6¼[[#28]]»v<va	Block	1
157.55.39.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
85.64.74.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.51.199.64	Ireland	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.51.199.64	Block	1
217.69.133.243	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter fb709480 in aka.idf.il/giyus/	None	1
123.59.59.52	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.elong.com/894-he/orchot.aspx	Block	1
109.67.118.47	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.142.68.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
2.53.21.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
154.98.212.168	Sudan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
81.218.53.114	Israel	147.237.72.156	aman.idf.il	Multiple _vti_ from 81.218.53.114	Block	1
212.150.245.250	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/112181.pdf	Block	1
46.19.85.168	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
201.55.56.118	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
96.233.178.243	United States	147.237.76.86	navy.idf.il	Malformed URL d±[[#27]]"[[ך´¸‰½ק•#1ע]]u[[#16]]hŒi6z¡![[#4]]¨ו 5•¿[[#23]]žµ[[ט#31Ù…]]ג-ıq¨ü•l^k[‹×]]8#[[]]41#[[z´ךˆcq-Ê·ג pn6¼[[#28]]»v<va	Block	1
88.80.184.136	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
169.229.3.90	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/rec.dat	Block	1
46.120.107.90	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
109.226.49.160	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
38.130.96.177	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
95.86.127.73	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
81.218.205.210	Israel	147.237.77.233	atal.idf.il	Suspicious Response Code	Block	1