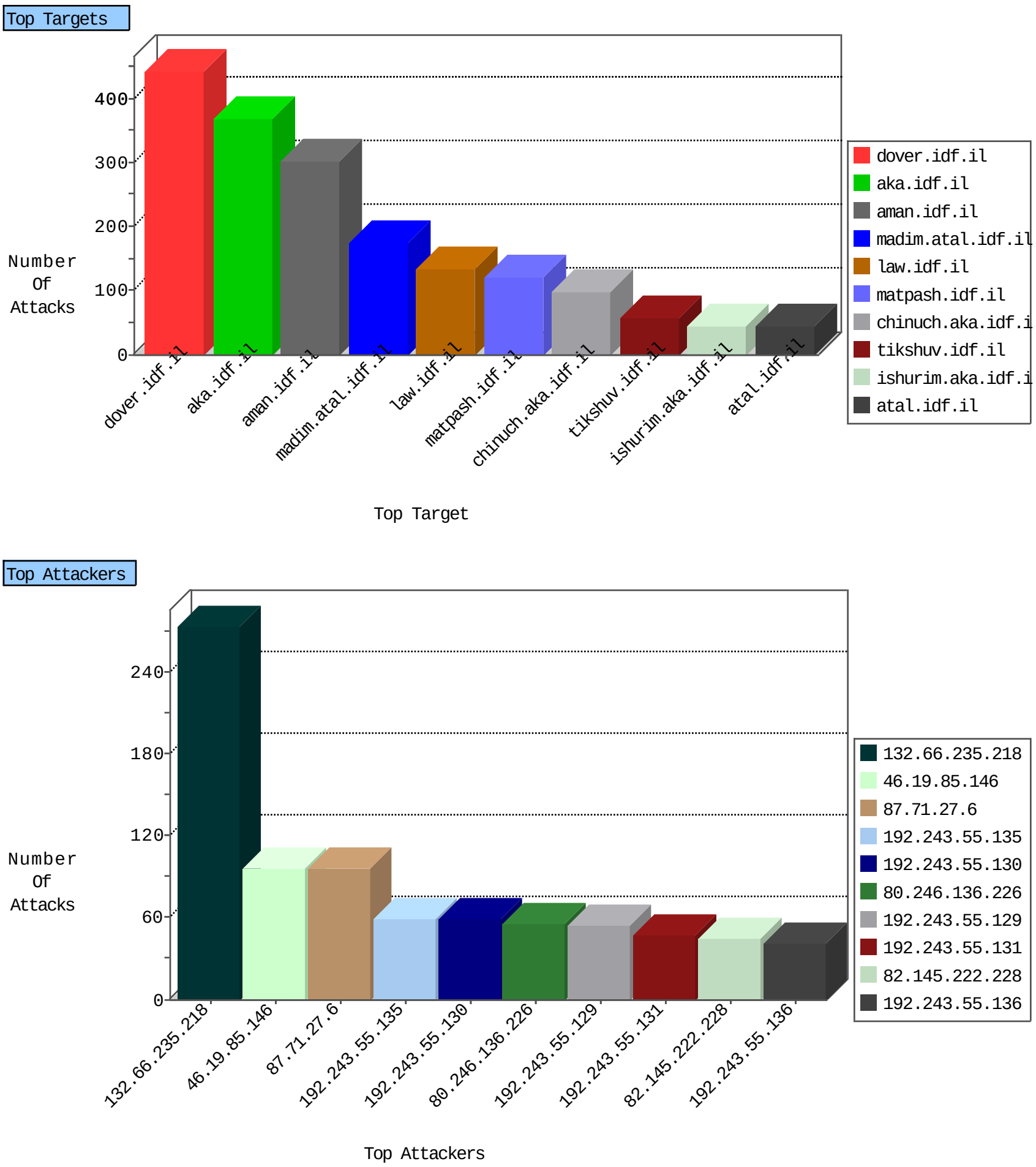
03-09-2016-18:04:03 to 03-09-2016-19:04:03

IDF Under Attack Daily Report



03-09-2016-18:04:03 to 03-09-2016-19:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.33	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	930
109.64.155.166	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	125
82.145.222.228	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	45
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	7
146.185.239.100	Russian Federation	147.237.72.156	aman.idf.il	block-sp-traf1	forward	2
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
94.159.168.196	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
213.57.142.54	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
5.29.193.19	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
82.166.68.171	Israel	147.237.0.35	akaws.idf.il	TCP handshake violation, first packet not syn	drop	1
10.0.0.22		147.237.77.233	atal.idf.il	Invalid TCP Flags	drop	1
79.178.58.112	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
87.71.133.32	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
212.179.90.106	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

03-09-2016-18:04:03 to 03-09-2016-19:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.241.234	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.183.179.152	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
217.70.44.165	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
67.228.38.74	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
67.228.38.74	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3
51.254.32.77	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
83.143.81.94	Norway	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
66.249.66.181	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	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	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-09-2016-18:04:03 to 03-09-2016-19:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
217.70.44.165	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
83.143.81.94	147.237.77.74	Norway	law.idf.il	SQL Injection - Select From	2
2.54.142.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.116.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.0.35	Canada	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
93.189.26.18	147.237.76.38	Austria	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.226.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.211.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.107.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.212.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.215.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.106	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.8.27	Sweden	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.181.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.36.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.0.35	Canada	akaws.idf.il	ET SCAN NMAP -f -sS	1
85.250.210.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
72.239.190.240	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.124.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.224.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
130.193.51.62	147.237.77.216	Russian Federation	dover.idf.il	portscan: TCP Distributed Portscan	1

03-09-2016-18:04:03 to 03-09-2016-19:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
132.66.235.218	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	108
132.66.235.218	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	107
87.71.27.6	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
132.66.235.218	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	45
176.13.19.191	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	32
79.182.16.193	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
129.98.194.114	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.32.167	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.147.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
147.236.34.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.66.10.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
109.67.48.47	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
185.89.217.234		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.52.37.111	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.217	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.33.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
109.67.248.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.103.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.87	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
185.89.217.230		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.184.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.21.16	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.32.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.153.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.130	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.120.124.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
81.218.153.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.89.217.230		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5

03-09-2016-18:04:03 to 03-09-2016-19:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
80.246.136.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
46.19.85.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
109.64.184.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.184.146	Block	4
46.19.86.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
132.66.235.218	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	3
176.13.7.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.11.126	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
37.26.148.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.70.75.96	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion $35 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	1
185.89.217.233		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.64.184.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
2.52.36.141	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.183.56.2	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
213.57.147.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
65.55.210.108	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.37	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
176.13.9.172	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
87.70.75.96	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion $42 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
71.227.52.133	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
112.198.103.181	Philippines	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
2.52.37.111	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
216.106.102.122	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.112	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/3/68633...	Block	1
46.19.85.37	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvs=56e0505d7002440e000; _pk_id.20.8afc=978a1da98fcfdd49.1457541215.1.1457541215.1457541215.; _pk_ses.20.8afc=*	Block	1
94.230.93.66	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	1
79.176.2.181	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163-5176-he/patzar.aspxborn-vagabond-where-have-you-been-all-myl-of-these-hitdreamsarticle&r=2&tmpl=blog	Block	1
112.198.103.181	Philippines	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
2.54.130.21	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
82.80.63.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kenesatuda/	Block	1
46.19.85.37	Israel	147.237.77.216	dover.idf.il	Malformed URL __atuvc=1	Block	1
185.89.217.227		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
94.230.93.66	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/xmlrpc.php	Block	1
79.178.35.203	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
208.115.113.89	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 208.115.113.89	Block	1
46.120.68.255	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	1
82.81.25.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
46.19.85.37	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method SP.NET_SessionId=rv3wjprgci1mg155yzf0ty55; in URL __atuvc=1	Block	1
185.89.217.232		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.182.16.193	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
212.150.195.192	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion $71 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.120.68.255	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1

03-09-2016-18:04:03 to 03-09-2016-19:04:03