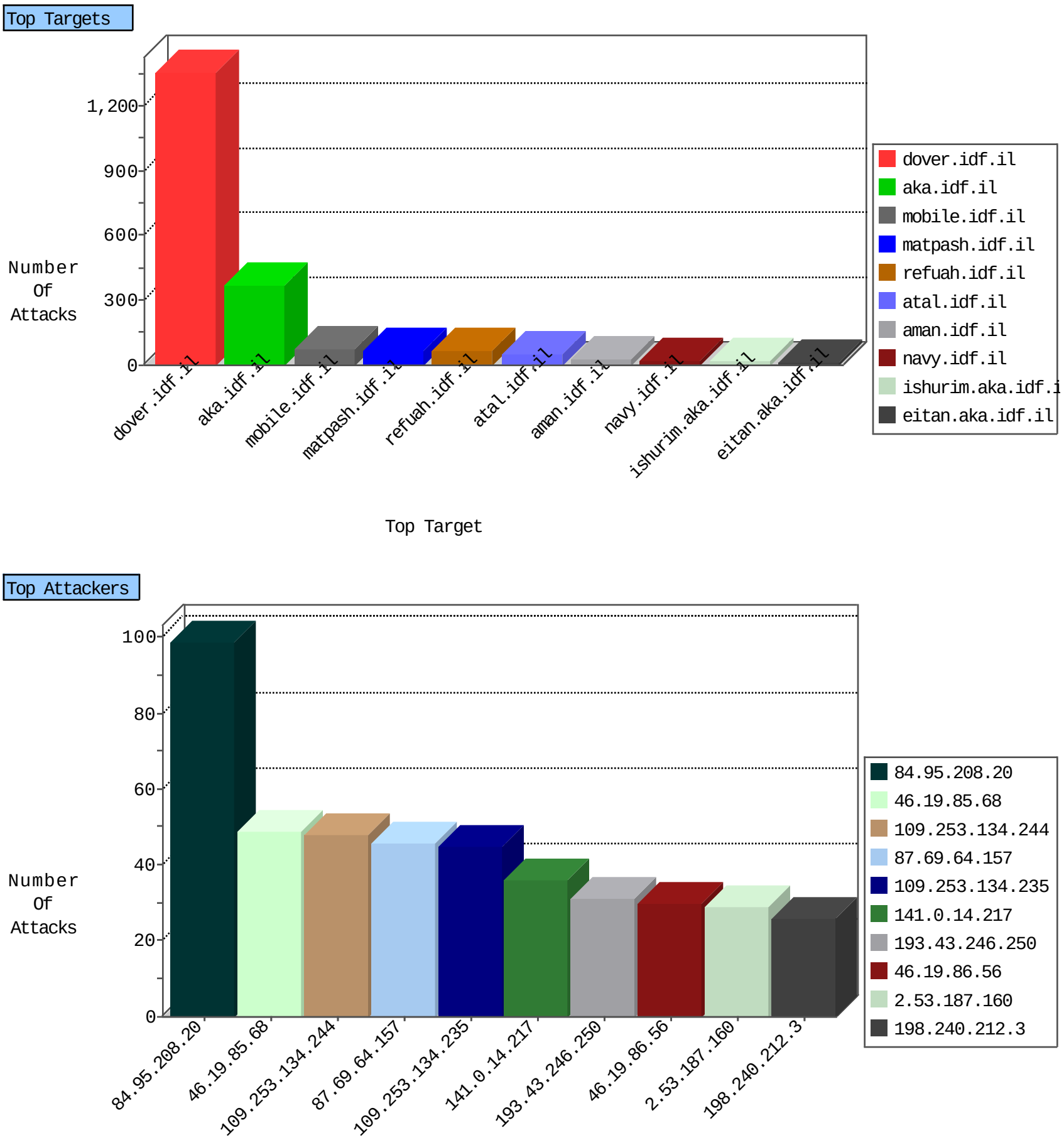
09-29-2016-11:04:04 to 09-29-2016-12:04:04

IDF Under Attack Daily Report



09-29-2016-11:04:04 to 09-29-2016-12:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.229	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
101.108.190.55	Thailand	147.237.72.217	e.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
198.44.110.12	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
109.253.199.223	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
198.44.110.12	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
217.69.133.223	Russian Federation	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
89.34.97.160	Romania	147.237.76.42	refuah.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Black List	drop	1

09-29-2016-11:04:04 to 09-29-2016-12:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.149.132.241	Italy	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
144.76.29.162	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
158.85.253.245	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

09-29-2016-11:04:04 to 09-29-2016-12:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.149.132.241	147.237.77.233	Italy	atal.idf.il	SQL Injection - Select From	16
158.85.253.245	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	3
194.90.134.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.153.198.249	147.237.77.121		e.navy.idf.il	ET SCAN Potential SSH Scan	1
106.120.209.150	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -f -sS	1
91.224.161.69	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
218.205.151.197	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
85.64.254.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.146.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.208.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.76.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.6.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.208.165.101	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
5.102.195.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.154.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.27.106.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
106.120.209.150	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.194	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.77.205	Ukraine	prisha.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
218.205.151.197	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -f -sS	1
81.218.195.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.71.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
201.7.217.250	147.237.76.147	Brazil	chinuch.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
31.223.182.178	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1

09-29-2016-11:04:04 to 09-29-2016-12:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.69.64.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
141.0.14.217	Europe	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	36
46.19.85.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
46.19.86.56	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
198.240.212.3	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
109.253.134.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	23
109.253.132.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
109.253.204.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.55.60.249	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
134.191.232.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.253.141.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.104	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
37.26.146.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.94.193.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
109.253.134.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
109.253.130.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
157.55.39.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
31.210.186.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.253.194.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
87.69.2.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.66	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
62.0.200.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
2.53.150.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
62.0.208.1	Israel	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.253.134.244	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
79.180.131.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.16.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.134.244	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
37.142.105.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.149.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.0.206.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.201	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.120.125.114	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	8
62.0.237.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.120.125.114	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
2.55.21.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.166.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7

09-29-2016-11:04:04 to 09-29-2016-12:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	48
121.9.124.190	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 121.9.124.190	Block	16
213.57.157.177	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.57.157.177	Block	9
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	9
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
5.196.154.234	France	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	7
31.154.81.48	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	7
121.9.124.190	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	6
109.253.144.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	5
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
185.32.179.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.81.160.69	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.81.160.69	Block	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
176.13.15.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.81.160.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	2
109.253.137.166	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/71772.pdf	Block	2
192.116.149.197	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/payslips/payslipslist.asp	Block	2
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
2.53.181.242	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal/site/templates/controller.asp	Block	2
109.253.143.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
2.53.16.152	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.101.202.67	Romania	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
2.53.185.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	2
109.253.130.100	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.76.45	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/m/	Block	1
195.16.161.75	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
84.111.233.36	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.154.81.48	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
2.53.51.129	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
157.55.39.127	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
109.253.134.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.176.67.163	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
213.8.124.118	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
84.109.183.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
46.16.141.50	Cyprus	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
185.120.125.114	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Method	Block	1
82.80.198.164	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.152.136	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
207.46.13.176	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/drushim/info.aspx	None	1
84.229.67.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.146.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.106.46.74	Palestinian Territory, Occupied	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	1
2.53.166.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-29-2016-11:04:04 to 09-29-2016-12:04:04