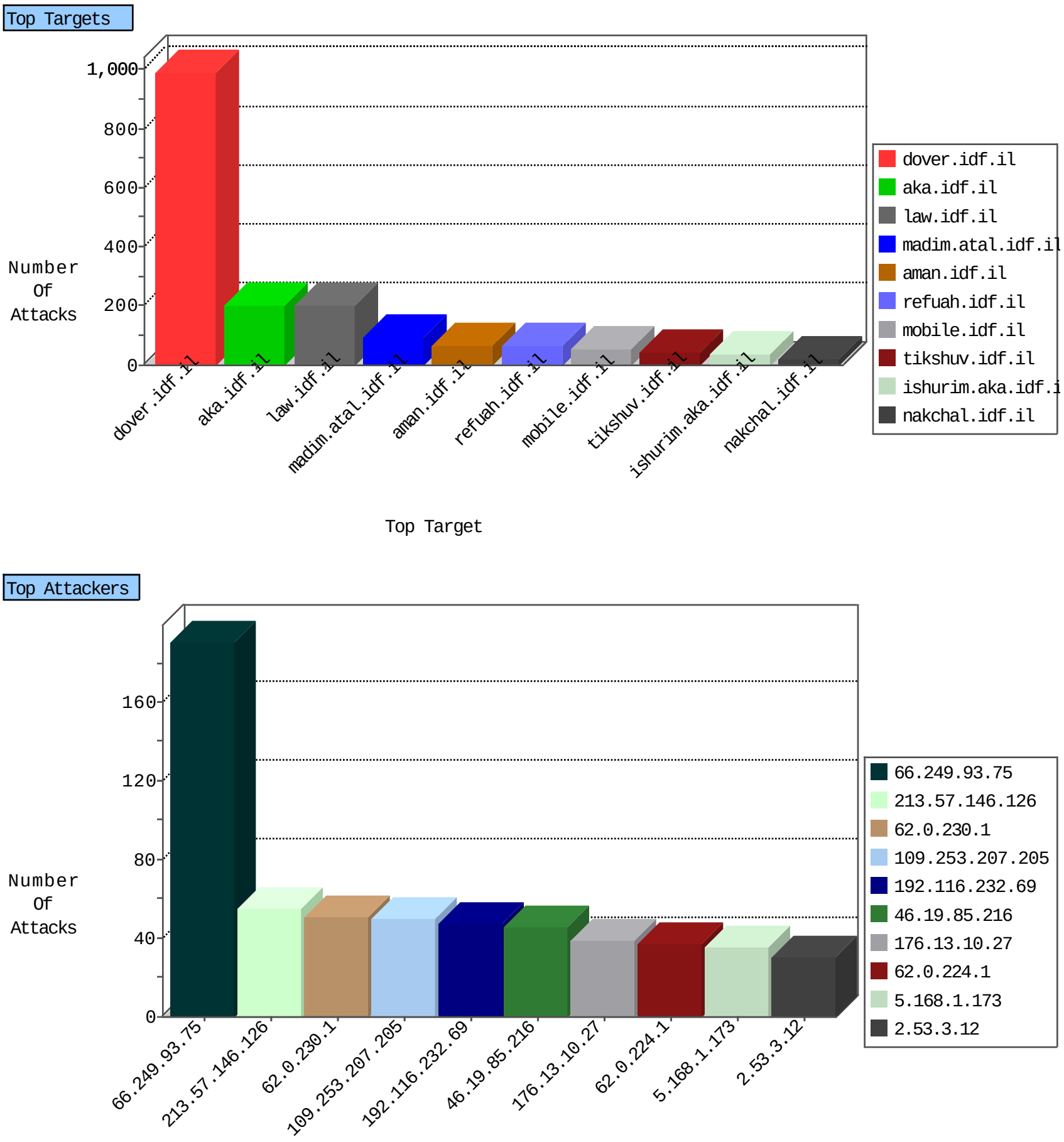
09-21-2016-09:04:01 to 09-21-2016-10:04:01

IDF Under Attack Daily Report



09-21-2016-09:04:01 to 09-21-2016-10:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
88.202.218.230	United Kingdom	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	28
213.8.50.49	Israel	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	14
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	10
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
208.110.84.68	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
209.126.102.181	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
209.126.102.181	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
45.32.205.133	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.31	nakchal.idf.il	Black List	drop	1
45.32.205.133	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
60.191.221.152	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

09-21-2016-09:04:01 to 09-21-2016-10:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.68.103	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-21-2016-09:04:01 to 09-21-2016-10:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.75	147.237.77.74	Europe	law.idf.il	ET SCAN NMAP -sA (2)	191
80.179.118.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
201.38.68.132	147.237.8.27	Brazil	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.116.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.116.247.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.138.222.199	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
128.232.110.28	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential SSH Scan	1
66.249.65.24	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
109.253.240.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
54.164.11.206	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
109.67.182.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
54.164.11.206	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.66.106.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.135.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.175.135	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.70.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.138.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.55.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
206.246.150.226	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.238.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.39.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.174.48	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
191.96.249.189	147.237.76.30	Chile	himush.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.83.162	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
54.164.11.206	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
109.253.132.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
54.164.11.206	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
109.67.103.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.189.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.188.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.30.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.57.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.108.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-21-2016-09:04:01 to 09-21-2016-10:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.230.1	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	51
109.253.207.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
62.0.224.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	37
5.168.1.173	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
2.53.3.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.86.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
46.19.85.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.19.85.216	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
46.19.85.216	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
2.53.169.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
155.250.255.143	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
2.53.136.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
185.24.207.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
213.57.146.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
213.57.146.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
213.57.146.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
213.57.146.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
213.57.146.126	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.86.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.86.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
84.109.115.57	Israel	147.237.0.34	tikshuv.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
2.53.140.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.85.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.246.138.117	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.86.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
212.179.126.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.120.74.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.20.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.41.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
100.92.19.64		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
213.8.50.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
89.139.171.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.128.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.213	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.102.242.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.0.232.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
85.130.219.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.213	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

09-21-2016-09:04:01 to 09-21-2016-10:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.10.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.19.85.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
192.116.232.69	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	17
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	16
192.116.232.69	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	14
80.246.138.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.67.251.183	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	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
109.253.215.79	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
77.139.168.138	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.168.138	Block	4
2.55.56.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
2.53.29.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
81.218.57.234	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
109.67.186.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	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
2.53.153.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.178.116.163	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.178.116.163	Block	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	2
81.218.57.234	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.57.234	Block	1
109.65.39.239	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
79.178.116.163	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/sachar	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
66.249.65.152	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
37.26.148.202	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
79.183.70.131	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
132.64.25.83	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.66.16	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
204.79.180.84	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
81.218.57.234	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/	Block	1
77.139.168.138	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
79.183.72.230	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.66.22	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/111452.pdf	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
207.46.13.63	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$Toche in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	1
79.177.1.102	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1

09-21-2016-09:04:01 to 09-21-2016-10:04:01