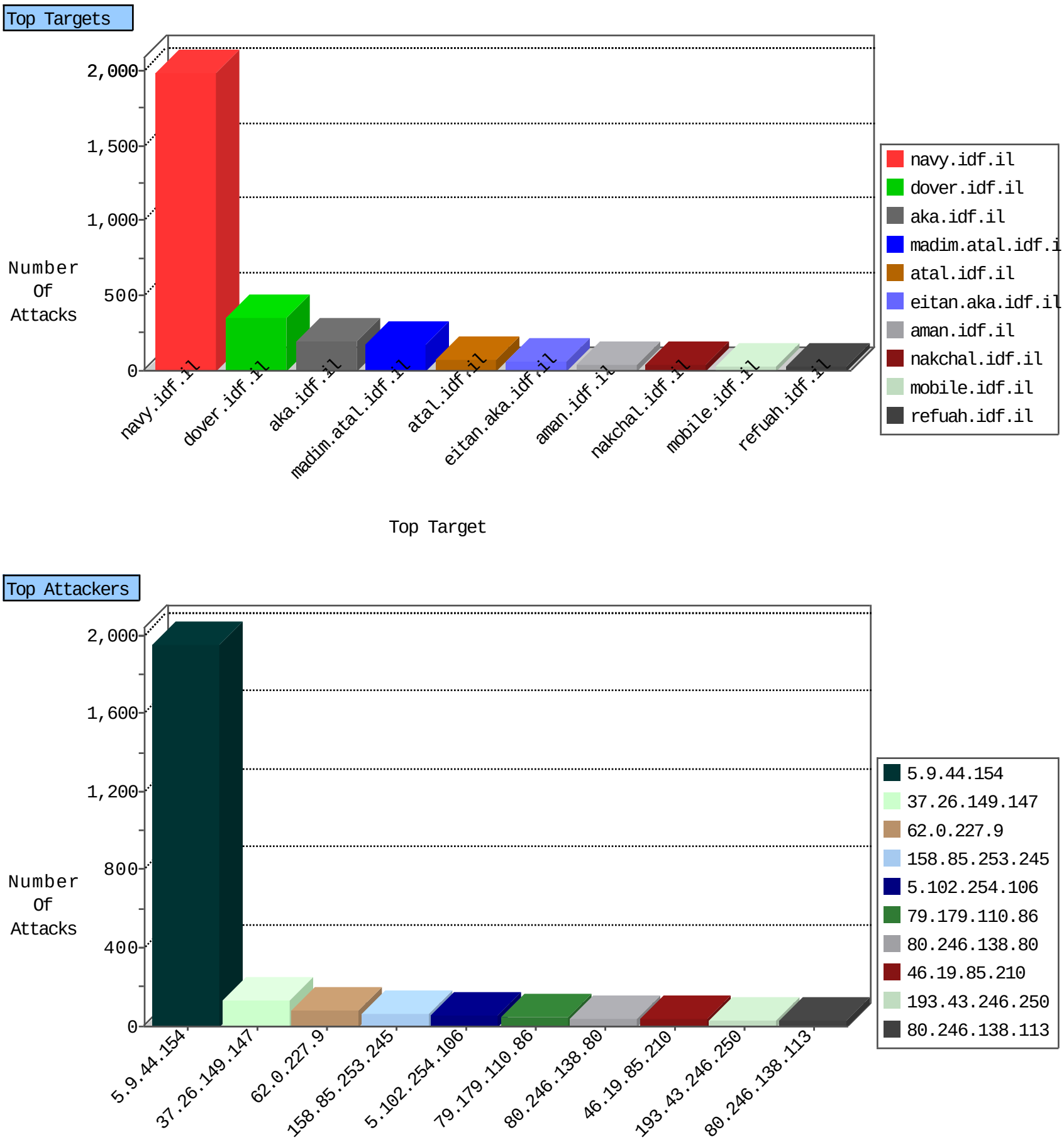
09-22-2016-13:04:00 to 09-22-2016-14:04:00

IDF Under Attack Daily Report



09-22-2016-13:04:00 to 09-22-2016-14:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.138.113	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	27
46.19.85.43	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
2.55.179.87	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.53.145.142	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
124.124.217.10	India	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
176.13.21.64	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
199.203.215.1	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
141.212.122.25	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
185.81.157.161	France	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

09-22-2016-13:04:00 to 09-22-2016-14:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
158.85.253.245	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
158.85.253.245	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
158.85.253.245	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
168.1.80.134	Australia	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
105.106.1.176	Algeria	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-22-2016-13:04:00 to 09-22-2016-14:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
158.85.253.245	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	27
168.1.80.134	147.237.77.233	Australia	atal.idf.il	SQL Injection - Select From	18
158.85.253.245	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	17
2.55.53.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.211.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.63.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
105.106.1.176	147.237.77.216	Algeria	dover.idf.il	SQL Injection - Select From	1
91.201.236.158	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
85.64.39.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.124.38.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.39.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.66	147.237.76.42	Europe	refuah.idf.il	ET SCAN NMAP -sA (2)	1
185.120.126.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.176.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
138.134.102.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.145.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.192.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.39.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
105.106.1.176	147.237.77.216	Algeria	dover.idf.il	GPL WEB_SERVER /etc/passwd	1
91.201.236.155	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.163.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.83	147.237.77.216	Europe	dover.idf.il	ET SCAN NMAP -sA (2)	1
194.114.146.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.60	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.24.228.20	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1

09-22-2016-13:04:00 to 09-22-2016-14:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1944
5.102.254.106	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52
62.0.227.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
79.179.110.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
62.0.227.9	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	27
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.85.210	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
74.91.23.166	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
100.92.214.61		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
17.78.79.113	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
80.246.138.80	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
109.253.129.202	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.243.150.195	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
31.168.142.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
213.111.134.43	Ukraine	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.246.138.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.192.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.7.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.138.80	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
74.208.192.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
82.166.219.240	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
80.246.138.80	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
80.246.138.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
80.246.138.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.237	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.210	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
180.183.122.170	Thailand	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
205.209.185.47	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
46.19.86.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.55.15.218	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
105.67.1.154	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.22.134.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
205.209.185.47	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
205.209.185.47	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
205.209.185.47	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
193.43.246.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
2.55.15.218	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.21.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.148.193	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.107	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.9.44.154	Germany	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
109.253.159.229	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.149.143	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

09-22-2016-13:04:00 to 09-22-2016-14:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	134
46.19.86.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
222.77.208.238	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 222.77.208.238	Block	17
46.117.44.147	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	6
222.77.208.238	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	5
77.138.207.221	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	4
109.64.1.212	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.80.196.44	Block	4
46.19.86.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
199.203.9.144	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	3
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.217.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.138.168.251	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
109.253.137.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
178.140.10.158	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
66.249.93.87	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
46.19.86.252	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
157.55.39.190	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/news/kamlar/mishpaha.jpg+	Block	1
91.199.119.17	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
46.18.20.35	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
109.253.192.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.102.242.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
188.161.25.85	Palestinian Territory, Occupied	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
68.180.228.44	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter PageNum in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
77.139.225.245	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/smalim/smalim.aspx	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Illegal Byte Code Character in Method H•H‰·j·v*‘[[#18]]‘Â[[#21]]	Block	1
66.249.79.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
109.253.211.41	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
46.19.86.252	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
37.26.147.248	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
68.180.230.216	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	1
46.188.72.194	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunsummary.aspx	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method •n¹•r‘FbÝr;[[#27]]i£"a#~[[#22]][[#17]]_*îúf¦bQò[[#2]]þ•¼tx[[#28]]¬Ÿ	Block	1
109.64.1.212	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
46.19.85.154	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.85.154	Block	1
79.180.61.19	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Unknown HTTP Request Method H•H‰·j·v*‘[[#18]]‘Â[[#21]] in URL	Block	1
66.249.93.83	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1
46.19.86.252	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
84.109.192.142	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
74.91.23.166	United States	147.237.72.156	aman.idf.il	Unauthorized Method HEAD for 147.237.72.156/	Block	1
199.203.152.210	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.102.8.215	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in URL	Block	1

09-22-2016-13:04:00 to 09-22-2016-14:04:00