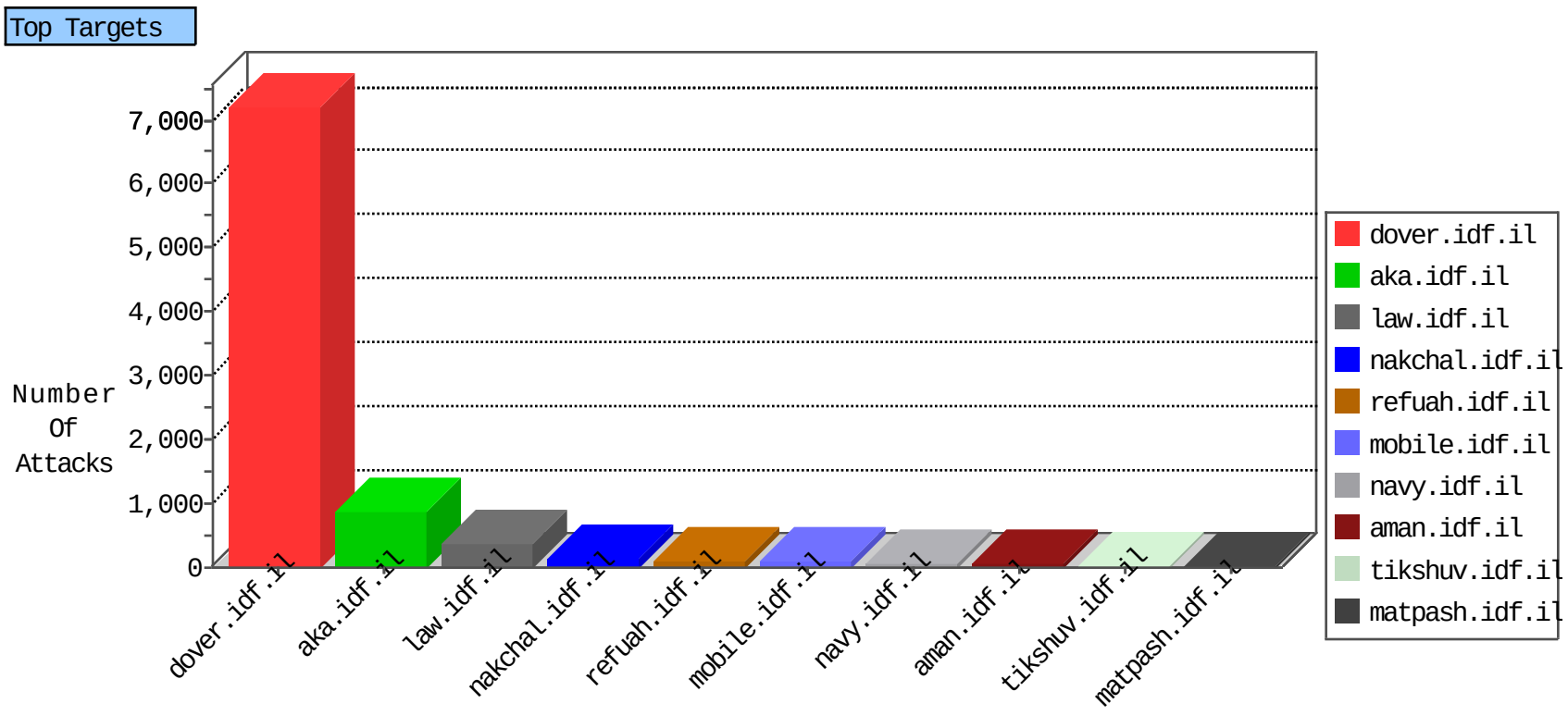
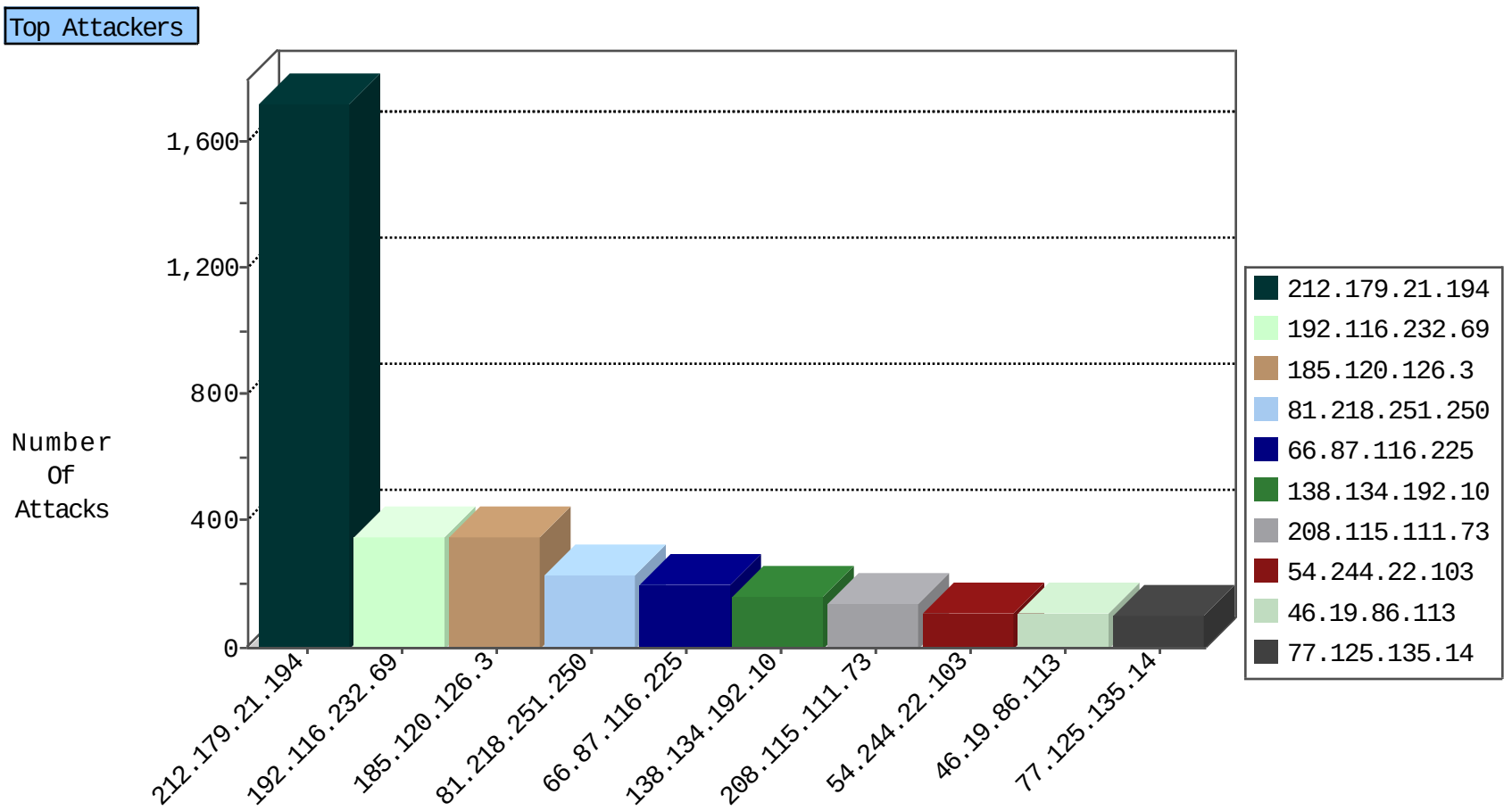
10-19-2015-13:04:07 to 10-19-2015-14:04:07

IDF Under Attack Daily Report





10-19-2015-13:04:07 to 10-19-2015-14:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.22	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2528
192.114.87.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	380
37.26.149.215	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	87
81.218.166.28	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
46.19.85.252	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
149.78.192.209	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
80.246.137.33	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
84.94.21.22	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
46.19.86.103	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
212.179.238.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
199.203.130.254	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.208.169	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.7.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
199.203.132.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
142.54.172.99	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	drop	1
149.78.141.112	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
46.19.85.8	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
107.150.55.53	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
46.19.86.103	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
5.8.202.76	Russian Federation	147.237.0.33	idf.il	L4 Source or Dest Port Zero	drop	1
107.167.112.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.26.148.197	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
173.208.168.165	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1

10-19-2015-13:04:07 to 10-19-2015-14:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-19-2015-13:04:07 to 10-19-2015-14:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.86.136	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
1.235.195.234	147.237.77.61	Korea, Republic of	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
185.32.179.81	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
119.90.18.5	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
109.65.125.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.65.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.130.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.252.197.194	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.85.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.194.195.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
1.235.195.234	147.237.77.61	Korea, Republic of	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
188.68.224.151	147.237.77.176	Poland	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
142.0.41.41	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
109.186.41.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.184.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.22.30	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
52.16.5.197	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.187.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.0.16	Sweden	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

10-19-2015-13:04:07 to 10-19-2015-14:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1713
185.120.126.3		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	348
81.218.251.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	229
66.87.116.225	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	185
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	138
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	111
46.19.86.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	109
77.125.135.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
185.26.180.32	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	100
199.203.132.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	91
2.54.32.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
195.93.234.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
80.246.133.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
69.234.177.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
46.19.85.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
2.52.29.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
82.81.129.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
195.242.191.45	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	47
212.199.57.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
109.152.226.50	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
212.199.103.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
212.116.166.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
146.185.58.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
81.218.198.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
212.143.133.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
78.40.176.178	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
2.54.188.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
81.218.208.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
100.100.2.93		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
185.69.144.33	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
37.26.146.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
132.64.162.32	Israel	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
82.80.203.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
46.19.85.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
79.177.222.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
62.24.252.133	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
80.246.130.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
84.109.76.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
46.19.86.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
193.5.216.100	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
93.173.61.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28

10-19-2015-13:04:07 to 10-19-2015-14:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.116.232.69	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	351
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	143
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	78
46.19.86.219	Israel	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1065-he/dover.aspx parameter SearchText	Block	65
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/67906.pdf	Block	65
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	52
212.143.133.107	Israel	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1065-he/dover.aspx parameter SearchText	Block	39
46.19.85.50	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	26
147.236.28.31	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
79.177.51.177	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
147.236.38.135	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	26
176.13.14.116	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
192.114.23.208	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	13
46.116.129.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
176.12.141.228	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in mobile.meitav.idf.il/1494-he/meitav.aspx	Block	13
2.54.15.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
85.65.15.215	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	13
213.57.61.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
66.249.93.132	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/shared/clientscripts/ui/ui.datepicker.js	Block	13
46.19.85.194	Israel	147.237.0.19	madim.atal.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 46.19.85.194	Block	13
180.76.15.144	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/a	Block	13
46.117.138.248	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.117.138.248	Block	13
176.12.143.218	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
2.54.191.161	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	13
91.230.79.254	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
66.249.93.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/ui/ui.datepicker.js	Block	13
46.19.85.252	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
185.21.121.113	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Multiple Abnormally Long Request from 185.21.121.113	Block	13
79.177.120.206	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/faqselection.aspx	None	13
199.203.240.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
46.117.138.248	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/https:/aka.idf.il/	Block	13
176.12.151.241	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 102 cookies	Block	13
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clienthttp/1.1 200 okdate: mon, 19 oct 2015 05:40:25 gmtlast-modified: sun, 03 jun 2012 07:44:40 gmtetag:	Block	13
109.165.12.81	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	13
46.19.86.104	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/shared/clientscripts/ui/ui.datepicker.js	Block	13
185.21.121.113	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 185.21.121.113	Block	13
149.88.233.9	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	13
79.179.56.155	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	13
212.116.166.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	13
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
46.19.85.50	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
176.13.9.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	13
132.64.162.32	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	13
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	13
188.165.15.89	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/iturim/asp/iturimpages.asp	Block	13
176.12.141.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	13
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13

10-19-2015-13:04:07 to 10-19-2015-14:04:07