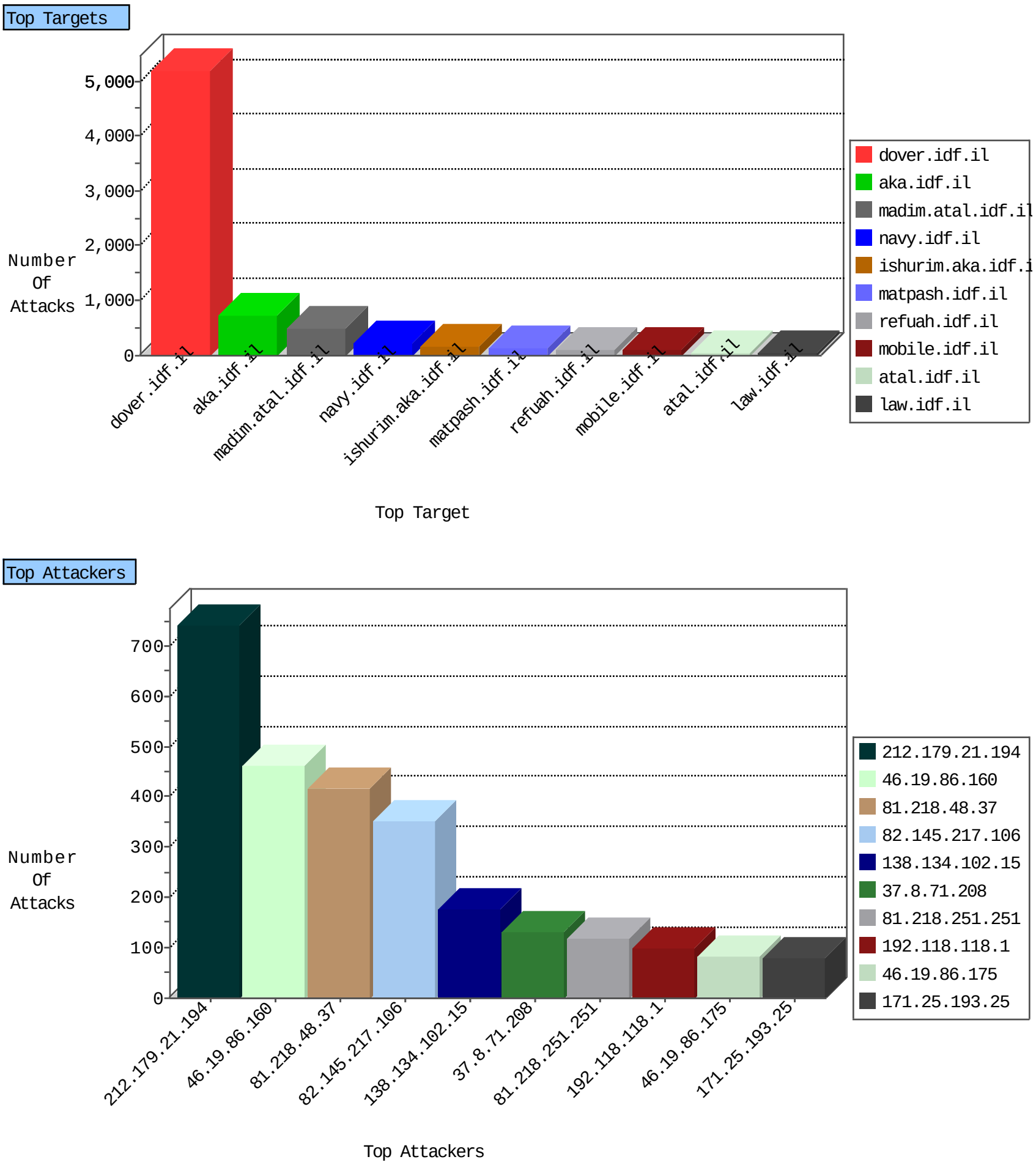
10-19-2015-09:04:03 to 10-19-2015-10:04:03

IDF Under Attack Daily Report



10-19-2015-09:04:03 to 10-19-2015-10:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.50.241	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	44
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	34
31.168.211.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
46.19.85.73	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
46.19.85.189	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	17
46.19.86.85	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	14
46.19.86.121	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
80.230.21.137	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.176.57.175	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
31.154.91.34	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.183.152.199	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.5.42	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
176.13.19.34	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
82.145.217.106	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
180.244.214.98	Indonesia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
89.139.177.180	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
37.8.71.208	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
93.174.93.146	Netherlands	147.237.76.202	e.halag.idf.il	Invalid TCP Flags	drop	1

10-19-2015-09:04:03 to 10-19-2015-10:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.227.211.186	United States	147.237.0.17	m.my-kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
37.142.68.7	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
51.254.130.59	United Kingdom	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
192.227.211.186	United States	147.237.0.17	m.my-kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
37.142.64.52	Israel	147.237.76.86	navy.idf.il	C008: HTTP: Xenu UserAgent	Block	1

10-19-2015-09:04:03 to 10-19-2015-10:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.19.85.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.1.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.36.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.160.240.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.140.62	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.96.28	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.56.0	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.57.209.110	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.77.216	United States	dover.idf.il	ET DROP Dshield Block Listed Source	1
193.105.134.220	147.237.77.61	Sweden	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
132.64.168.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
79.143.180.44	147.237.77.205	Germany	prisha.idf.il	ET SCAN NMAP -sS window 1024	1

10-19-2015-09:04:03 to 10-19-2015-10:04:03

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	724
81.218.48.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	418
82.145.217.106	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	351
37.8.71.208	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
81.218.251.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	117
192.118.118.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	99
46.19.86.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
171.25.193.25	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
46.120.71.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
77.158.88.40	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
46.19.85.214	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
81.218.71.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
140.242.217.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
194.90.156.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
80.178.204.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
195.160.240.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
46.19.86.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
89.138.60.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
169.252.4.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
176.13.19.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
46.19.86.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
180.244.214.98	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
89.139.63.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
79.179.107.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
79.177.27.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
212.199.244.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
46.19.85.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
176.12.142.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
80.246.133.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
176.12.136.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
79.176.1.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.86.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
138.134.102.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
91.231.192.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.42.2.106	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20

10-19-2015-09:04:03 to 10-19-2015-10:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.160	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.160	Block	455
138.134.102.15	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 138.134.102.15	Block	143
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	78
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	52
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	39
192.118.78.201	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	39
176.13.3.164	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1744	Block	39
192.118.78.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	26
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
46.19.85.35	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	26
176.13.6.215	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	13
138.134.102.15	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	13
2.54.133.215	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in aka.idf.il/main/sachar/tfasim.aspx	None	13
108.175.9.107	United States	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	13
79.182.57.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17841-en/dover.aspx maj. gen. gadi eizenkot appointed deputy to chief of general staff	Block	13
176.12.149.107	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	13
109.65.43.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
31.154.172.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
85.64.97.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
2.52.26.66	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	13
212.150.66.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files	Block	13
185.32.179.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
151.80.31.141	Italy	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	13
2.54.157.114	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
108.175.9.107	United States	147.237.77.74	law.idf.il	eMail Hoarding	Block	13
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	13
192.118.78.200	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
176.13.2.50	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	13
109.226.44.128	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	13
212.179.227.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
85.130.244.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
2.52.62.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
188.143.232.19	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 188.143.232.19	Block	13
77.125.78.23	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	13
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	13
171.25.193.25	Sweden	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	13
2.54.179.91	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	13
108.175.9.107	United States	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	13
66.249.93.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyu	Block	13
109.226.44.128	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	13
46.19.86.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
2.54.6.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
212.199.57.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
93.172.49.215	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$chkBitulTlushim in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	13
188.143.232.19	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/searchresults/searchresults.aspx/templates/sendtofriend/sendtofriend.aspx	Block	13
77.125.163.206	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	13
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/style/1.he/scroller/skin.css	Block	13
176.12.146.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13

10-19-2015-09:04:03 to 10-19-2015-10:04:03