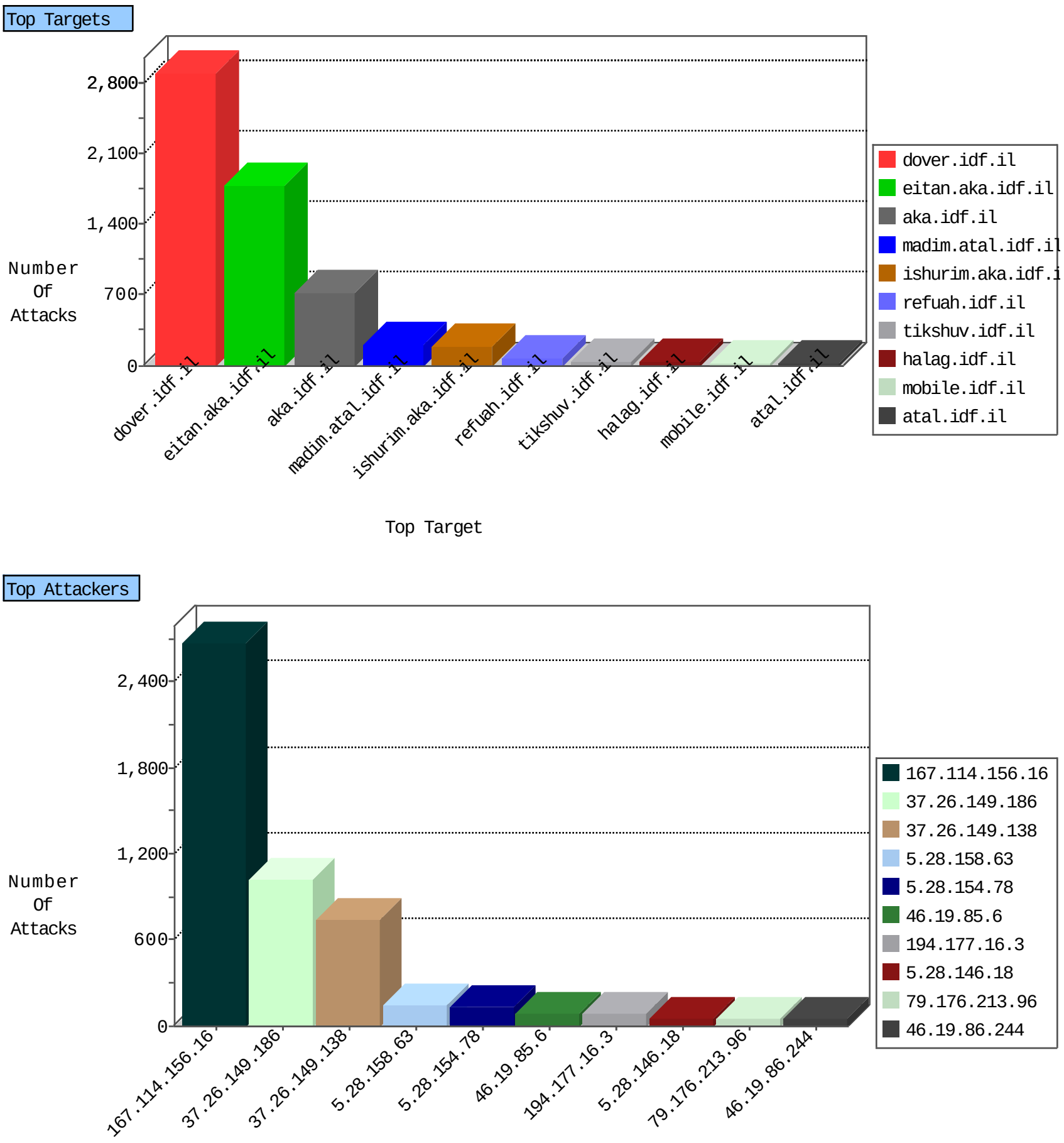
12-09-2015-14:04:02 to 12-09-2015-15:04:02

IDF Under Attack
Daily Report



12-09-2015-14:04:02 to 12-09-2015-15:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3467
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
79.181.2.140	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
192.118.132.185	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3

12-09-2015-14:04:02 to 12-09-2015-15:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-09-2015-14:04:02 to 12-09-2015-15:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	3
137.226.113.7	147.237.76.86	Germany	navy.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1
91.218.246.103	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN NMAP -sS window 1024	1
77.126.87.103	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.102.217.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.154.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
122.114.17.100	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
80.246.137.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.194.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.197.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.131.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.27.105.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-09-2015-14:04:02 to 12-09-2015-15:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.149.186	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	927
37.26.149.138	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	561
194.177.16.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	81
5.28.158.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	66
5.28.154.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	65
5.28.154.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	65
5.28.158.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	65
92.239.176.150	United Kingdom	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
46.19.86.138	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	43
46.19.86.163	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
82.81.32.141	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
5.28.146.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
5.28.146.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	19
5.28.146.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
213.57.134.144	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
46.120.28.230	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
213.57.134.144	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
46.19.86.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.178	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.6	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.12.147.46	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.29.197.144	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
5.28.158.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
46.19.86.153	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
2.54.20.15	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
88.76.195.88	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
213.8.90.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
84.229.156.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
195.200.205.78	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.185.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.114	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
183.13.124.174	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
192.114.91.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.117.134.240	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.70.66.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.36.76	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.128	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.146.160	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
84.111.152.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.146.160	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.179.142.99	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4

12-09-2015-14:04:02 to 12-09-2015-15:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.138	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	187
37.26.149.186	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.149.186	Block	100
46.19.86.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
46.19.85.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	47
46.19.85.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
207.241.226.39	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.241.226.39	Block	22
2.54.149.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.85.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
79.180.198.231	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.180.198.231	Block	10
176.12.136.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
176.12.140.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
207.241.226.39	United States	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	7
176.12.136.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	6
79.176.213.96	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.176.213.96	Block	5
79.176.213.96	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 79.176.213.96	Block	5
45.55.184.19		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 45.55.184.19	Block	4
79.176.213.96	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 79.176.213.96	Block	4
79.176.213.96	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.176.213.96	Block	4
79.176.213.96	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.176.213.96	Block	3
79.176.213.96	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 79.176.213.96	Block	3
46.19.85.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.167.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.161.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.213.96	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 79.176.213.96	Block	3
2.54.55.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.213.96	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.176.213.96	Block	3
81.17.31.222	Switzerland	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.176.213.96	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 79.176.213.96	Block	2
176.13.3.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.5.14	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
79.176.213.96	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 79.176.213.96	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
78.111.186.38	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.111.186.38	Block	2
37.26.146.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
137.226.113.7	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/yesthisisareallylongrequesturlbutwearedoingitonpurposewearescanningforresearchpurposepleasehavealookattheuseragentthxyesthisisareallylongrequesturlbutwearedoingitonpurposewearescanningforresearchpurposepleasehavealookattheuseragentthxyesthisisareallylongrequesturlbutwearedoingitonpurposewearescanningforresearchpurposepleasehavealookattheuseragentthx	Block	1
2.52.162.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
194.153.113.35	Germany	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
46.120.28.230	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
95.86.71.188	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/1048-7486-he/tikshuv.aspx&sa=u&ved=0ahukewjrkaai5s7jahvf6g4khz2wb9kqfggimaa&usg=afqjcnhf5bpjxko81dkznynqlftw3lnosg	Block	1
79.176.213.96	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method ?Â,Â•_Â‰RPKÃŠÃ¬Â¿Â› Â£R[tÃ²4Â°Ã?hÃŒKÃ…Ã»ÂŽÂ†Ã¨iÂ?a+Â'Ãƒ0Ã´Â,ZÂ'xxÂ½Ãƒ x7R^Â°FÂ Â°KÂ«Â¨!{A4%Ã§Â²Ã—Ã¢Â¯Ã°{!$Â«Ã†Ã¡^Ã?9Ã^Y[[#31]]Ã€ÂˆÃŒ Â½Ã¥ÂŒÂ¾Â‰[[#26]]Â»Ã'Â¤Ã˜kÂ ÃŒÂ©s,[[#1]]cÂ' [[#12]]<Â°O_Â½[[#2]]}6NÃ?dÂ?`lÃ—	Block	1
176.12.147.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
41.188.105.9	Mauritania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
5.29.197.144	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1133-he/atal.aspx	Block	1
79.176.213.96	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method ?Â,Â•_Â‰RPKÃŠÃ¬Â¿Â›Â£R[tÃ²4Â°Ã?hÃŒKÃ…Ã»ÂŽÂ†Ã¨iÂ?a+Â'Ãƒ0Ã´Â,ZÂ'xxÂ½Ãƒ x7R^Â°FÂ Â°KÂ«Â¨!{A4%Ã§Â²Ã—Ã¢Â¯Ã°{!$Â«Ã†Ã¡^Ã?9Ã^Y[[#31]]Ã€ÂˆÃŒ Â½Ã¥ÂŒÂ¾Â‰[[#26]]Â»Ã'Â¤Ã˜kÂ ÃŒÂ©s,[[#1]]cÂ' [[#12]]<Â°O_Â½[[#2]]}6NÃ?dÂ?`lÃ— in URL 3×³×"Â¨j[[#6]]×´Â¼×™ Â®knÂ¸â€ Ö·[[#1]]n×™Â½f[[#6]]a>]×'[[#29]]×¦Â?c[ÂŠÂ´×³	Block	1
217.132.26.226	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
66.249.79.25	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
173.176.152.157	Canada	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1

12-09-2015-14:04:02 to 12-09-2015-15:04:02