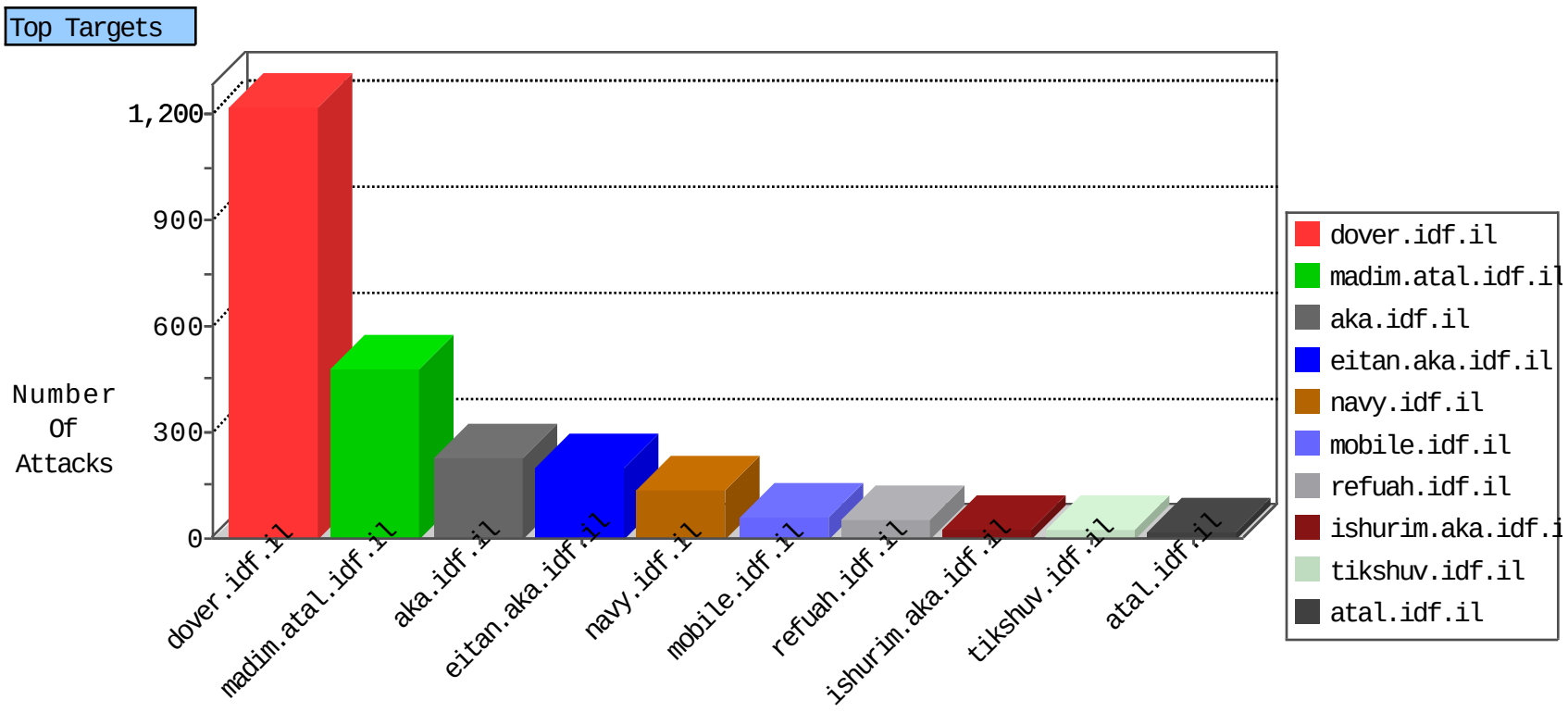
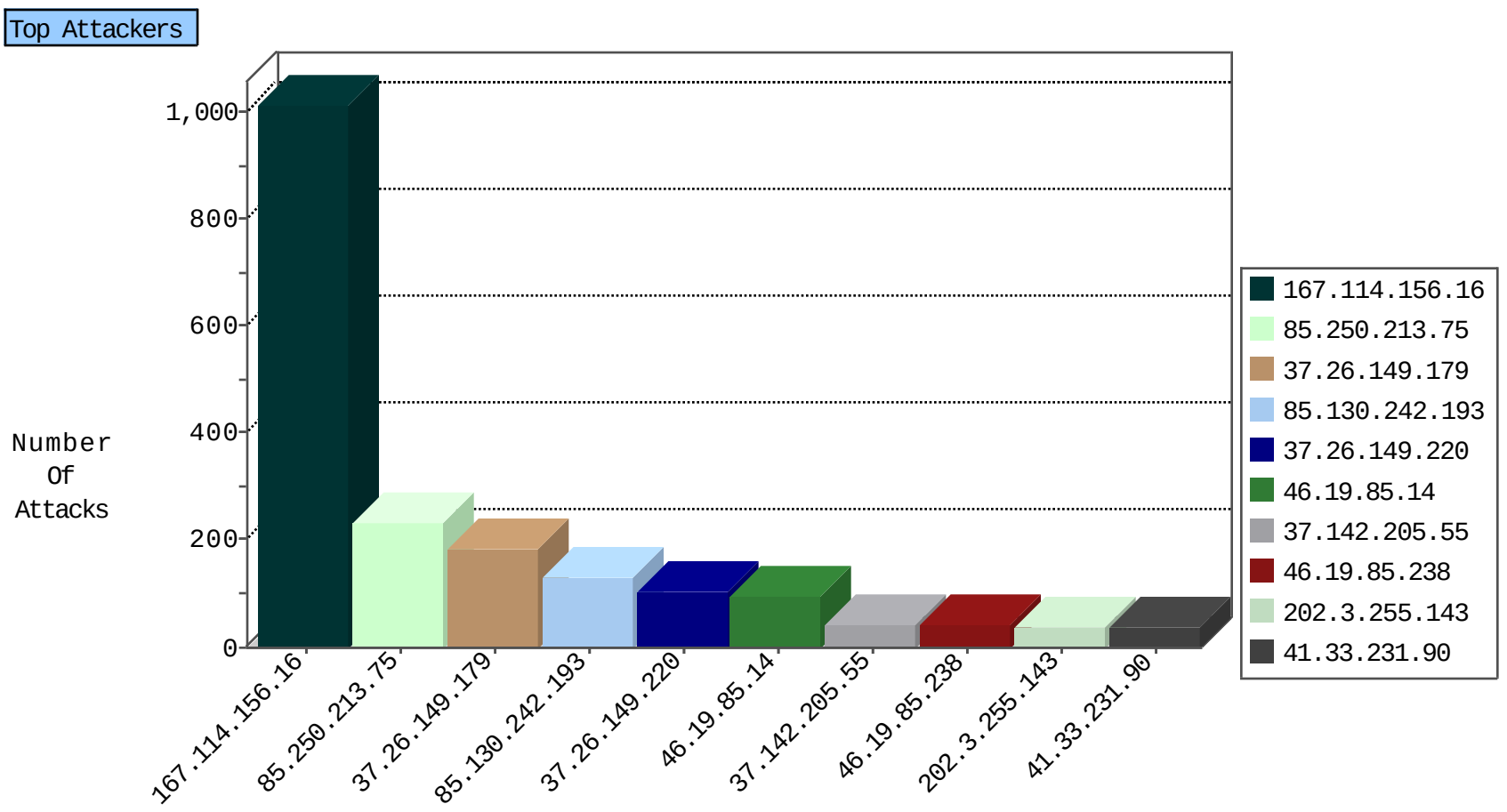
01-16-2016-22:04:07 to 01-16-2016-23:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-16-2016-22:04:07 to 01-16-2016-23:04:07

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	3000
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
202.112.51.96	China	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
180.212.223.35	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
66.102.9.10	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
202.112.51.96	China	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
180.212.223.35	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
45.32.183.57		147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
202.112.51.96	China	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
202.112.51.96	China	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
66.249.93.180	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
223.114.38.89	China	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
202.112.51.96	China	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
180.212.223.35	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
45.32.183.57		147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
202.112.51.96	China	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
202.112.51.96	China	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
142.54.160.212	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
202.112.51.96	China	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
180.212.223.35	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
46.166.188.68	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
202.112.51.96	China	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
202.112.51.96	China	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
45.32.183.57		147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

01-16-2016-22:04:07 to 01-16-2016-23:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-16-2016-22:04:07 to 01-16-2016-23:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

01-16-2016-22:04:07 to 01-16-2016-23:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.149.220	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
46.19.85.14	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
85.130.242.193	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
85.130.242.193	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	40
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
85.130.242.193	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	36
85.130.251.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.142.205.55	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
46.19.86.108	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
37.142.205.55	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	19
66.249.64.250	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.183.70.9	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.120.129.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.69	Israel	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
41.238.217.108	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
84.228.202.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.142.64.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
176.13.23.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.26.149.220	Israel	147.237.8.45	e.eitan.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.102.254.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.29.131.215	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
31.154.166.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.238.217.108	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
84.109.152.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.120.251	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.238.217.108	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
194.90.198.147	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
79.181.225.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.20.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.126.12		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.39.7	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.52.150.240	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
176.13.8.245	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.69	Israel	147.237.0.16	my-kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
154.103.114.218	Sudan	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.120.219.148	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.238.190.53	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.143	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
41.238.190.53	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
199.30.25.226	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
85.130.242.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.230.86.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.130.242.193	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.57.189.32	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence		monitor	4
41.238.217.108	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

01-16-2016-22:04:07 to 01-16-2016-23:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.213.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	157
37.26.149.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
85.250.213.75	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 85.250.213.75	Block	74
37.26.149.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	71
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
46.19.86.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
77.127.78.98	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 77.127.78.98	None	5
46.116.168.141	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
95.86.80.56	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 95.86.80.56	Block	4
104.131.221.134	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	4
37.26.149.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	4
46.19.86.229	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
176.13.23.169	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
5.28.188.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.21.134	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.13.21.134	Block	3
93.172.37.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.166.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.127.61.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.129.110	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.228.202.248	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.142.64.102	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.20.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
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	2
85.64.96.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.183.147.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.21.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.136.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.18.18.203	Palestinian Territory, Occupied	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20050529.htm	Block	1
202.112.51.96	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to www.ebay.com/	Block	1
76.103.147.77	United States	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method Accept: in URL text/html	Block	1
5.102.254.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.80.115	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.35.142.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/asp/personalentrance.asp	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
69.58.178.59	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
5.28.156.61	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
109.253.220.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.230.230.230	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
87.69.215.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.166.228.10	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
207.46.13.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/registrationwizard/register.aspx	Block	1
77.126.171.125	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
37.26.147.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.83.183	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized Method HEAD for www.chinuch.aka.idf.il/894-he/chinuch.aspx	None	1
209.40.95.254	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
85.64.22.51	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
37.142.205.55	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1

01-16-2016-22:04:07 to 01-16-2016-23:04:07