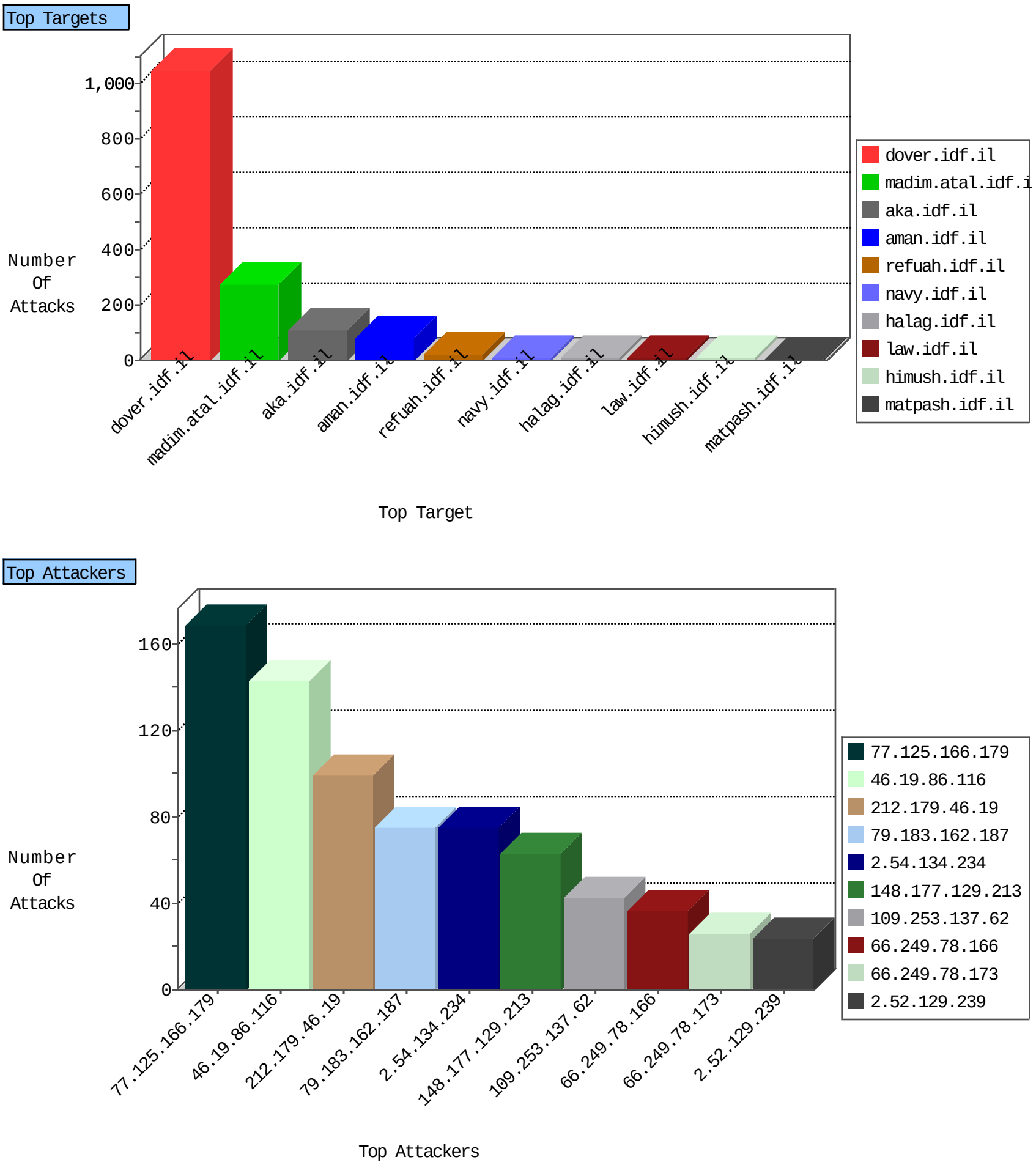
04-14-2015-15:03:01 to 04-14-2015-16:03:01

IDF Under Attack
04-14-2015-15:03:01

Top Targets



Top Attackers

04-14-2015-15:03:01 to 04-14-2015-16:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2977
122.176.12.3	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	482
41.89.229.17	Kenya	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
176.12.142.87	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.28.155.17	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
103.231.118.245		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

04-14-2015-15:03:01 to 04-14-2015-16:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.120.63.116	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
80.248.161.32	Finland	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
77.127.27.28	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
41.220.69.168	Nigeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.137	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.179.8.169	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.180.58.165	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
2.52.159.81	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
2.54.190.24	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
109.64.109.121	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1

04-14-2015-15:03:01 to 04-14-2015-16:03:01

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.93.253	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	2
82.166.158.100	Israel	147.237.76.86	navy.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	2
61.240.144.66	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
52.4.127.156	United States	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
207.232.28.187	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
101.226.179.84	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
5.29.131.140	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.46.19	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
193.106.54.37	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
91.217.90.49	Ukraine	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1

04-14-2015-15:03:01 to 04-14-2015-16:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
77.125.166.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	169
212.179.46.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	98
148.177.129.213	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	63
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
2.52.129.239	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
46.19.86.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
176.10.104.234	Switzerland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
62.219.143.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
194.90.99.129	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
46.116.106.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
192.116.98.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
31.168.100.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
79.179.8.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
82.166.158.100	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
66.249.73.231	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
80.74.121.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
147.236.30.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
79.178.147.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
220.255.1.116	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
79.176.129.208	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
80.74.126.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.116.74.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
212.179.155.129	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
205.204.93.131	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
109.253.147.60	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
95.86.102.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
79.182.28.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
41.89.229.17	Kenya	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
193.239.108.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.19.85.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.120.63.116	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	7
141.201.219.161	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
167.88.16.81		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
203.127.96.252	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.64.150	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.140.106	Israel	147.237.0.19	madim.atal.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.86.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
213.57.225.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.86.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
207.46.13.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
185.24.204.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.116	Block	143
2.54.134.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	75
109.253.137.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
81.218.48.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	11
79.183.162.187	Israel	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 79.183.162.187	Block	6
79.183.162.187	Israel	147.237.72.156	aman.idf.il	Multiple Malformed URL from 79.183.162.187	Block	6
79.183.162.187	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 79.183.162.187	Block	6
213.151.35.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
79.183.162.187	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 79.183.162.187	Block	6
79.183.162.187	Israel	147.237.72.156	aman.idf.il	Multiple Illegal HTTP Version from 79.183.162.187	Block	5
79.183.162.187	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.183.162.187	Block	5
79.183.162.187	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Value from 79.183.162.187	Block	5
79.183.162.187	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Header Line from 79.183.162.187	Block	5
79.183.162.187	Israel	147.237.72.156	aman.idf.il	Multiple Malformed HTTP Header Line from 79.183.162.187	Block	4
79.183.162.187	Israel	147.237.72.156	aman.idf.il	Multiple NULL Character in Header Name from 79.183.162.187	Block	4
66.249.65.41	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.65.41	Block	4
109.253.157.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
79.183.162.187	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in URL from 79.183.162.187	Block	4
109.64.98.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
79.176.180.111	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/6_s3_	Block	3
185.32.179.191	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
149.88.86.62	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
213.8.242.98	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
188.120.148.221	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
77.125.163.150	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.125.163.150	Block	3
85.65.72.127	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.72.127	Block	3
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	3
46.19.85.240	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
79.183.102.243	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
81.199.120.169	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
80.246.130.103	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/giyus	Block	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
93.172.151.73	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.10.104.234	Switzerland	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 176.10.104.234	Block	2
85.65.72.127	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/6_s3_	Block	2
80.246.139.215	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
61.135.190.198	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
79.183.162.187	Israel	147.237.72.156	aman.idf.il	NULL Character in Method [[#12]][[#1]]4'[[#7]]ÂŽ zÂ¨[[#18]]PPD[[#20]]C[[#11]]b]<ÃžgdÂ=hÃ›Â°ÂŸS'[[#0]]Â?Ã†Â¯g~[[#7]]Âµ0ÂŒ Â°]Ã¥-Ã½Â³+Ã¯APÃºÃ–Â‹Ã·UÂ¿#Ã»Ã©ÃžÃ¨ÃœUÃ—Â†x-!ÂœÃ˜%ÂžÂ™ MÃºb[-l:Â¦V)Â–Â¶V[[#15]]Â±=Â›p[[#15]]X7Ã¤[[#22]]Ã Ã?vÂ¡ÃŒ Â©BEÂ®[[#20]]>Â“Â²7Â³Â¼IÂ‹_5@[[#11]][[#5]]Ã?Â‰~Â?ÃŸKÃ§j:&Ã¬Ã·	Block	1
79.178.30.141	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
123.30.128.71	Vietnam	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
66.249.81.208	United States	147.237.76.30	himush.idf.il	URL is Above Root Directory www.chimush.atal.idf.il/../favicon.ico	Block	1
109.65.59.116	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.186	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/801-he/patzar.aspx	Block	1
84.94.192.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/×?×™×©×•×¨×™×?	Block	1
79.183.162.187	Israel	147.237.72.156	aman.idf.il	Illegal HTTP Version •Âªtmt%Â†[[#16]]JÃ¯Â¥Ã•Â“•Ã¡~~Ã•[[#18]]->[[#26]]vÃ¡Ã“ Â¶ÃŸÂºÃ²[[#1]]Â·•Ã²ÃŽÃ™qÂ°JQÃ¬C[[#14]]Ã¼]Ã›Â¥3Â²[[#6]]ÂœÂŒ [[#8]][[#22]]wÃ”[[#27]]ÂŸ8Â^Â±Â?RÂ?owcÃ”[[#23]][[#1]]hÃƒaÃ–Â– ri[[#31]]Â©Ã•[[#29]]wÂ»[[#5]]Ã§ÂŒf[[#15]]1~r[[#30]][[#3]] Ã¥Â¤Â?JÃ±<#Â?Ã˜ [[#5]]Ã • Ã¢1[[#27]]k~Ã?[[#4]]Âº[[#27]]Ã¦Ã^ÂŠÂ?Â¾]Â?vÂ¯Ã´Â?EÃ¶Ã¢Ã?Ã–Â” [[#5]]ÂŸ.Â±Â¼%[[#21]]4Ã¡Ã¬rXoÂ¤_[[#23]][[#22]][[#2]]Ã?ÃœÂ€rÂ˜Ã–Â?4Â, OMU[[#24]]Â½[[#22]]Ã¡CÃŸM[[#7]]Â¥\Ã€Ã”bÂœÂ›<[[#18]]Â€-qÂªÂ´e/Â¼Âƒ tÂ©ÃŒÃ?[[#26]]&-ÂºÃ·[[#4]]Ã?ÃžLÃ‹Ã†Ã¸=Â·@OÂ	Block	1
192.115.97.253	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
176.12.140.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.22	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
80.230.39.236	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
78.193.250.123	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1