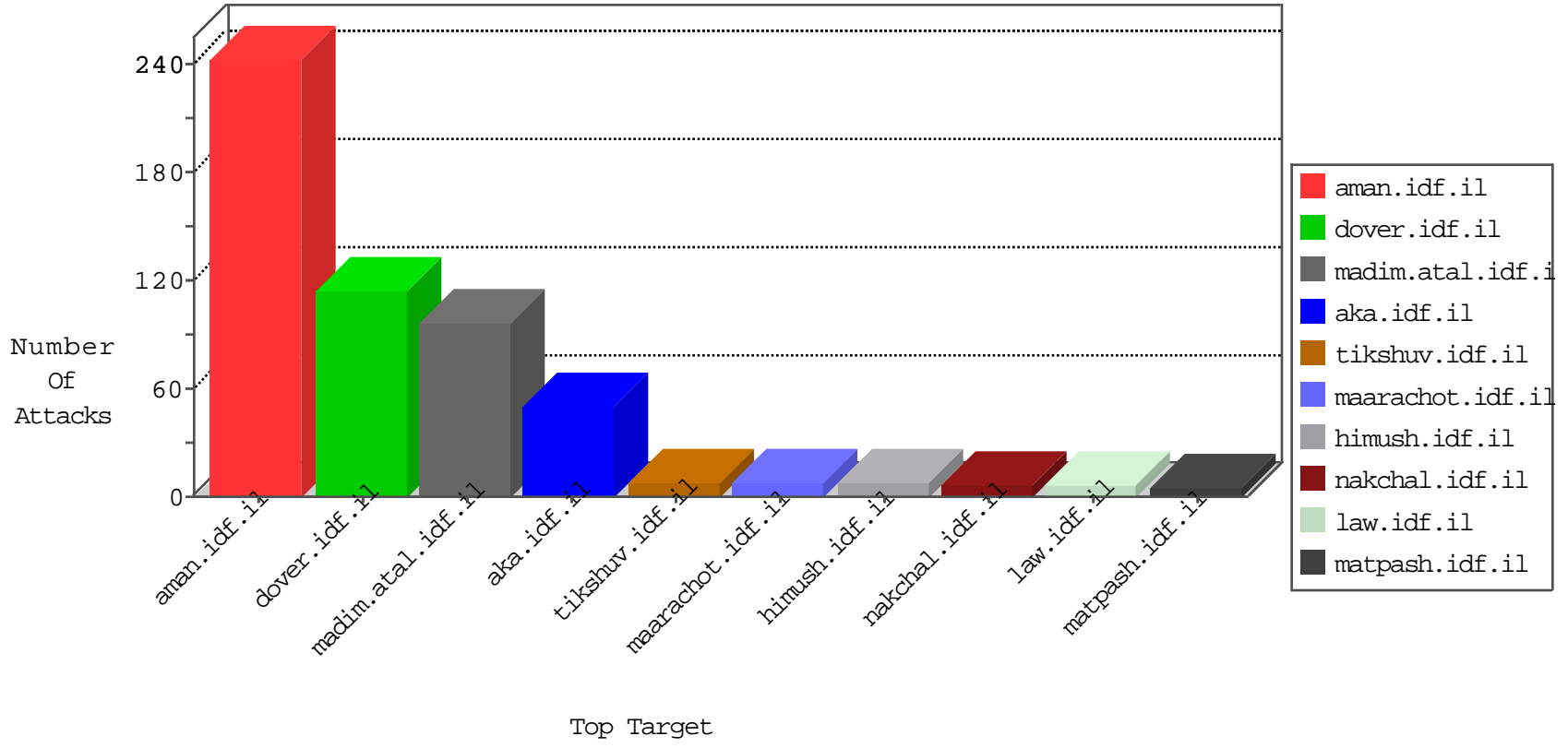
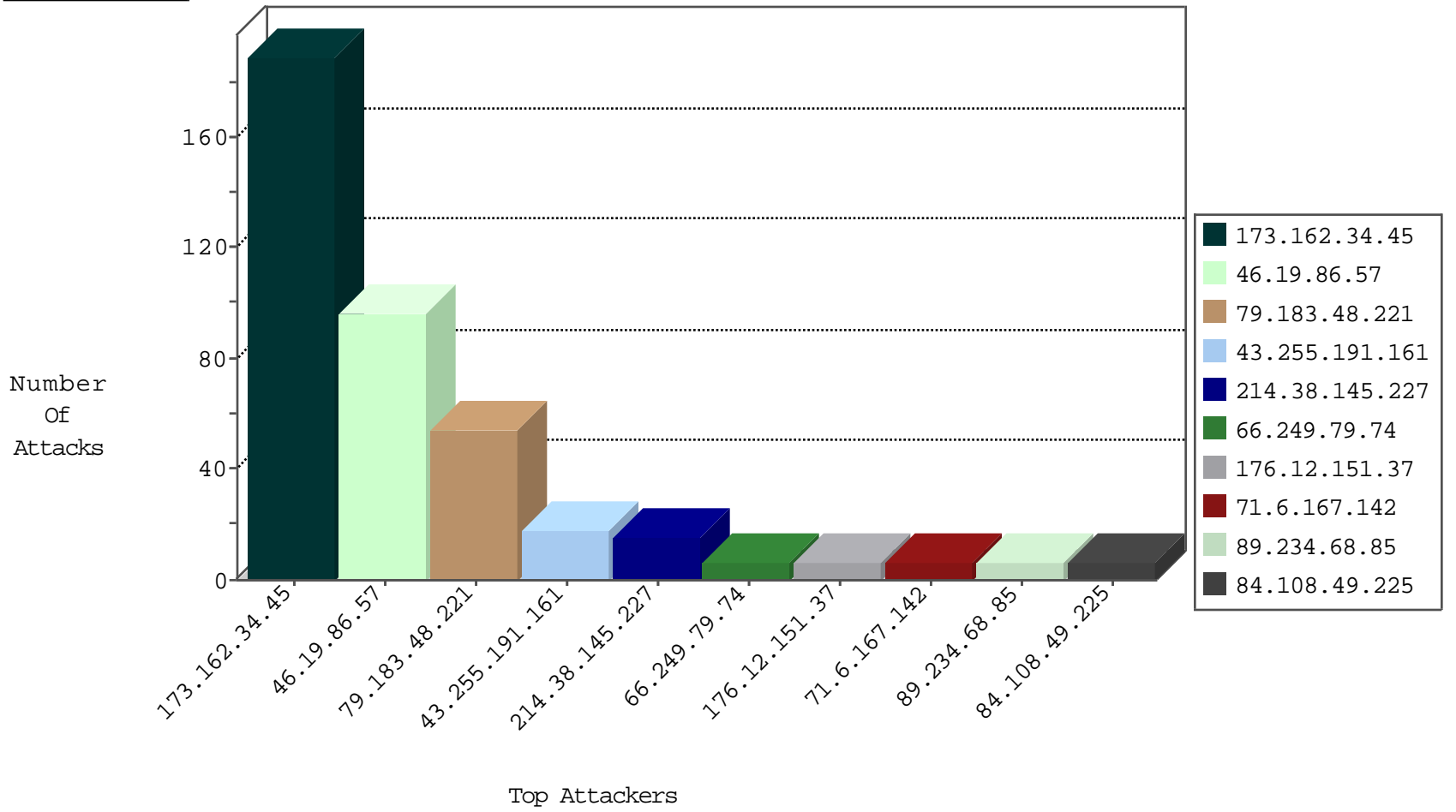




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
173.162.34.45	United States	147.237.72.156	aman.idf.il	TCP Scan (vertical)	drop	1190
79.183.48.221	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	873
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
173.162.34.45	United States	147.237.72.156	aman.idf.il	Frk_Under_Attack_Con_Tcp	drop	7
46.19.86.106	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
66.249.93.235	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
192.116.55.216	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
66.249.93.238	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
141.138.156.16	France	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
46.121.121.227	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
141.138.156.16	France	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
195.37.190.86	Germany	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
82.102.141.250	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.248.165.134	Netherlands	147.237.77.170	maarachot.idf.il	Frk_Under_Attack_Con_Tcp	drop	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
173.162.34.45	United States	147.237.72.156	aman.idf.il	C1000155: HTTP: OPTIONS methods	Permit	2
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	2
84.111.138.55	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	2
85.25.43.94	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
79.177.119.52	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
41.130.235.26	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.178.125.2	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.254	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
109.65.59.218	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	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

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
173.162.34.45	United States	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	4
89.234.68.85	Ireland	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.93.179	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
2.54.130.187	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
94.159.222.131	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
173.162.34.45	United States	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
43.255.191.161	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
43.255.191.161	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
85.108.18.245	Turkey	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.161	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
45.63.48.126		147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
85.108.18.245	Turkey	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.161	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.195	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
81.200.91.2	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
199.255.137.52	United States	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
81.200.91.2	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
178.19.107.114	Poland	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
173.162.34.45	United States	147.237.72.156	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.240.144.67	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
43.255.191.161	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
173.162.34.45	United States	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.67	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
43.255.191.161	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.76.34	yochalan.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.14	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
85.108.18.245	Turkey	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.161	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
212.47.236.90	France	147.237.76.198	e.yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
81.200.91.2	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.161	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
214.38.145.227	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
176.12.151.37	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
84.108.49.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
31.186.228.24	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
87.68.25.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
38.117.168.5	United States	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
109.67.114.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
77.125.250.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.67.141.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
178.69.81.140	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
198.48.92.104	United States	147.237.76.202	e.halag.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
98.248.47.127	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
77.125.246.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
31.186.228.26	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
173.162.34.45	United States	147.237.72.156	aman.idf.il	SAM rule	drop	drop	1
89.108.159.50	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
201.234.230.209	Venezuela	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
31.186.228.66	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
176.12.139.98	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
90.227.238.158	Sweden	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
5.29.45.160	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
212.76.127.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
79.181.123.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
37.142.74.184	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
94.242.221.68	Luxembourg	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
5.29.93.246	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
109.253.136.205	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
38.111.147.86	United States	147.237.0.34	tikshuv.idf.il		drop	drop	1
95.86.77.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.79.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
111.103.20.11	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.57	Block	95
173.162.34.45	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	12
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple NULL Character in Method from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple Abnormally Long Header Line from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple Malformed HTTP Header Line from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple Malformed URL from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple NULL Character in Header Name from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Distributed Illegal HTTP Version	Block	9
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple NULL Character in Url from 173.162.34.45	Block	7
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	6
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	5
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in URL from 173.162.34.45	Block	4
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	4
109.253.145.6	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	4
79.182.113.191	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	4
109.66.191.19	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
77.125.77.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
93.172.173.21	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	2
66.249.93.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
85.65.53.237	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
93.173.148.99	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	2
80.246.139.233	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.178.126.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
213.57.184.167	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
162.243.89.33	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 162.243.89.33	Block	2
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Value from 173.162.34.45	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
173.162.34.45	United States	147.237.72.156	aman.idf.il	Abnormally Long Header Line request header name	Block	1
109.253.132.35	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
173.162.34.45	United States	147.237.72.156	aman.idf.il	NULL Character in Header Name at	Block	1
85.64.132.237	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
173.162.34.45	United States	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Value	Block	1
66.249.73.136	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
176.228.133.125	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/gyus/authenticationonservice.aspx/getuserdetails	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.133.141	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
173.162.34.45	United States	147.237.72.156	aman.idf.il	Abnormally Long Request method	Block	1
109.253.141.123	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
173.162.34.45	United States	147.237.72.156	aman.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#1]][[#1]][[#0]][[#1]]w[[#3]][[#3]]U:@[#14]]oÃ³ÂœUÃžÃšÂ¿</[#18]]Ã•Â«mÃ«Ã«Ã„Ã¼Ã-Ã~ÃœPÃ™Ã¬Ã·ÃeÃša[[#0]][[#0]]Ã†[[#0]][[#5]][[#0]][[#4]][[#0]][[#2]][[#0]][[#8]][[#0]][[#20]][[#0]][[#3]][[#0]][[#1]][[#0]][[#21]][[#0]][[#6]][[#0]][[#22]][[#0]][[#23]][[#0]]3[[#0]]9[[#0]][[#25]][[#0]]]:[[#0]][[#26]][[#0]][[#24]][[#0]]5[[#0]]	Block	1
79.178.19.231	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan	Block	1
173.162.34.45	United States	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#1]][[#1]][[#0]][[#1]]w[[#3]][[#3]]U:@[#14]]oÃ³ÂœUÃžÃšÂ¿</[#18]]Ã•Â«mÃ«Ã«Ã„Ã¼Ã-Ã~ÃœPÃ™Ã¬Ã·ÃeÃša[[#0]][[#0]]Ã†[[#0]][[#5]][[#0]][[#4]][[#0]][[#2]][[#0]][[#8]][[#0]][[#20]][[#0]][[#3]][[#0]][[#1]][[#0]][[#21]][[#0]][[#6]][[#0]][[#22]][[#0]][[#23]][[#0]]3[[#0]]9[[#0]][[#25]][[#0]]]:[[#0]][[#26]][[#0]][[#24]][[#0]]5[[#0]]	Block	1
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1206-en/cogat.aspxcoordination	Block	1
178.69.81.140	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.40	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14363-he/dover.aspx	Block	1
2.133.151.238	Kazakistan	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1116-en/dover.aspx	Block	1