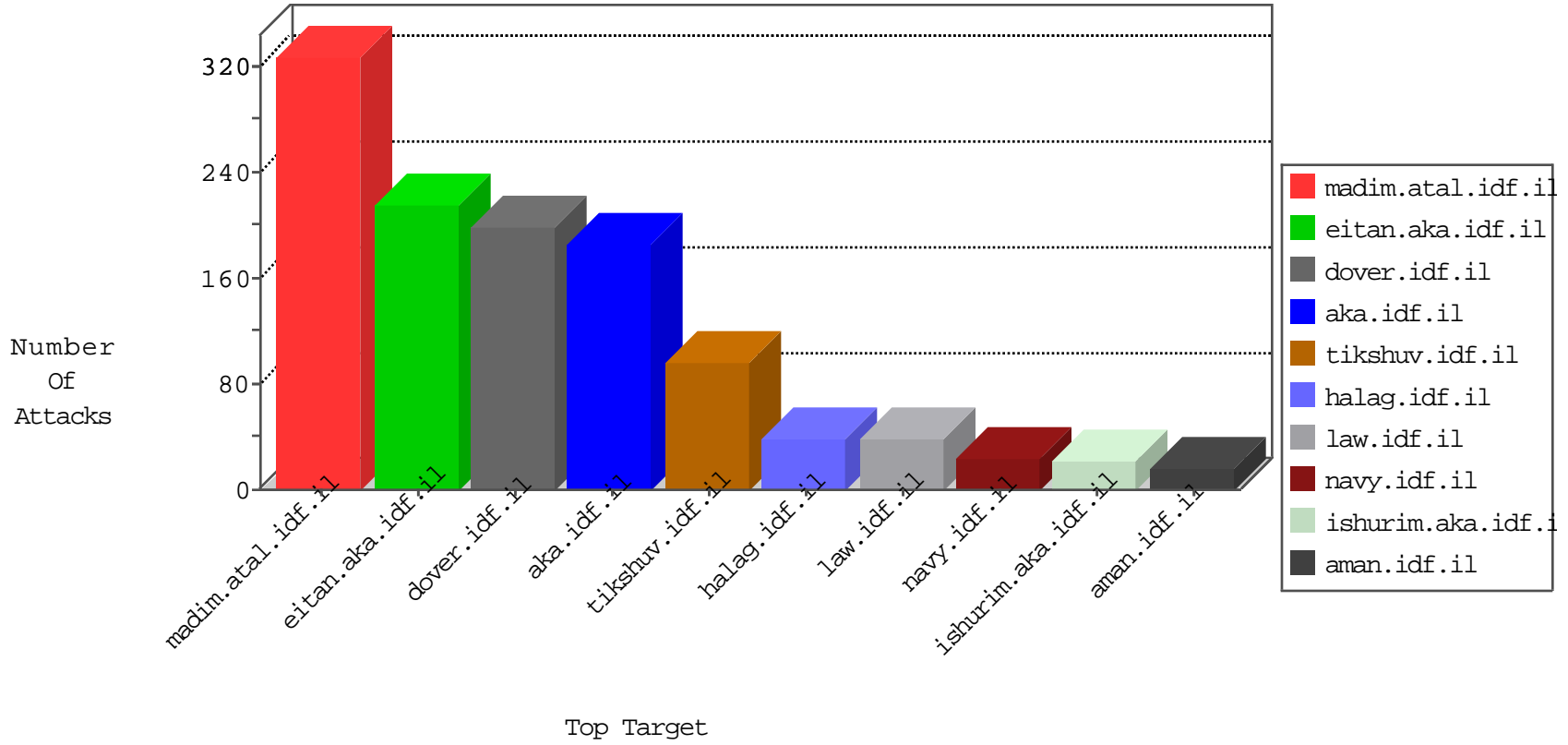


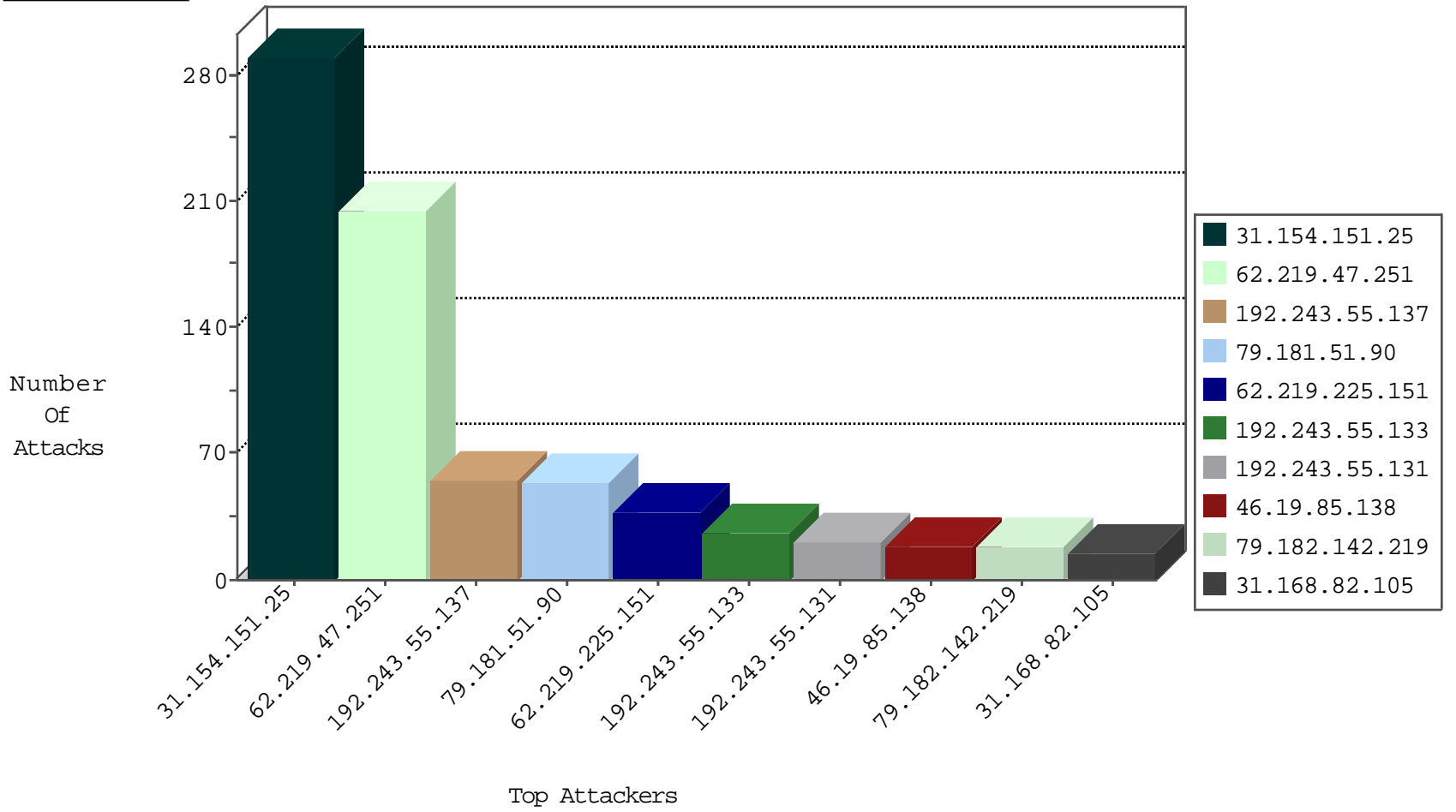
# IDF Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
82.145.221.237	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3
76.114.170.22	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
78.187.175.100	Turkey	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
122.150.183.36	Australia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
173.52.245.163	United States	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.82.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
79.181.51.90	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
109.65.32.109	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.19.86.10	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
176.13.2.18	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.181.242.166	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.26.148.133	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.26.149.146	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.96	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
85.250.148.136	Israel	147.237.72.167	ishurim.aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.93.27	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.177	China	noore.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
213.136.91.26	147.237.76.148	Germany	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
79.178.113.83	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
213.136.91.26	147.237.77.205	Germany	prisha.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.219.47.251	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	195
79.181.51.90	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
62.219.225.151	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.85.161	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.98	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.137.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.182.142.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.183.201.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.142.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.23.158	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.182.142.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
62.219.225.151	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
87.69.193.248	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.250.115.252	Finland	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.137	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
213.57.183.111	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.172.86	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.178.213.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.165.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.1.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.41.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.186.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.175.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.209.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.52.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.47.251	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.63.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.3.144.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.179.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.103.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.158.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-04-2016-15:04:04 to 03-04-2016-16:04:04

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.177.190.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.154.151.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	287
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
79.179.23.197	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 79.179.23.197	None	8
213.57.208.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
85.64.20.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.196.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.127.15.83	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.127.15.83	Block	3
37.236.8.80	Iraq	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.236.8.80	Block	3
87.70.82.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.20.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.68.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.19	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.127.15.83	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
95.86.96.4	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/&sa=u&ved=0ahukewjk0oiflqflahxckq8khq6od54qfggimaa&sig2=fuj7hjlkqo4tri34eczyr&usg=afqjcnhcvyyg7w1cq-yhd5_a mmzoyodtwa	Block	2
207.46.13.107	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
197.115.237.171	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/admin	Block	1
74.82.47.2	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
60.242.192.67	Australia	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Illegal Byte Code Character in URL	Block	1
37.60.47.78	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
212.227.81.200	Germany	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 212.227.81.200 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
212.227.81.200	Germany	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
64.39.109.20	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method y045ohaygb45 in URL	Block	1
213.8.204.18	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
5.29.240.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct151 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
212.227.81.200	Germany	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL "f+kŽ•[s Ū[[#16]]-...[[#29]] oÊihwzý †\ "a•x -'	Block	1
84.111.80.75	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
199.30.24.95	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
62.219.47.251	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Abnormally Long Request method	Block	1
212.227.81.200	Germany	147.237.72.166	aka.idf.il	NULL Character in Header Name at kK•êi[[#8]]Eƒo^[[#24]]bôæ°äufse^ÆQ[[#0]]¼È'è èSi5×Ê@[[#5]]'k(®^[[#23]]]İ¥E{#I[[#28]]}f[[#12]]'çFEŪó•EmA@Ñóai...,M9Y!¼,[[#28]]Y™*«³f'O±AS Øý...p-n"FG[[#14]]d;¹'á{?X?[[#24]]]±[[#20]]èö4GÖ)ÖJö[[#28]]]ç<¼&`èA[[#27]]]ç±0[[#12]]üŪ•sy%Jü-ä[[#16]]]ô•yİ,~--[[#16]]] [[#18]]]F.SÁ"t[[#21]]]ä, 'Ñ´ôDç_	Block	1
156.198.49.91		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
79.182.131.166	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
212.227.81.200	Germany	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	1
197.115.237.171	Algeria	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Abnormally Long Request method	Block	1
46.19.86.77	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
5.29.240.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct199 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
212.227.81.200	Germany	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
62.219.225.151	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in Method	Block	1
156.198.83.97		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.227.81.200	Germany	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.183.201.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/gyus	Block	1
212.227.81.200	Germany	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
197.115.237.171	Algeria	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 197.115.237.171	Block	1