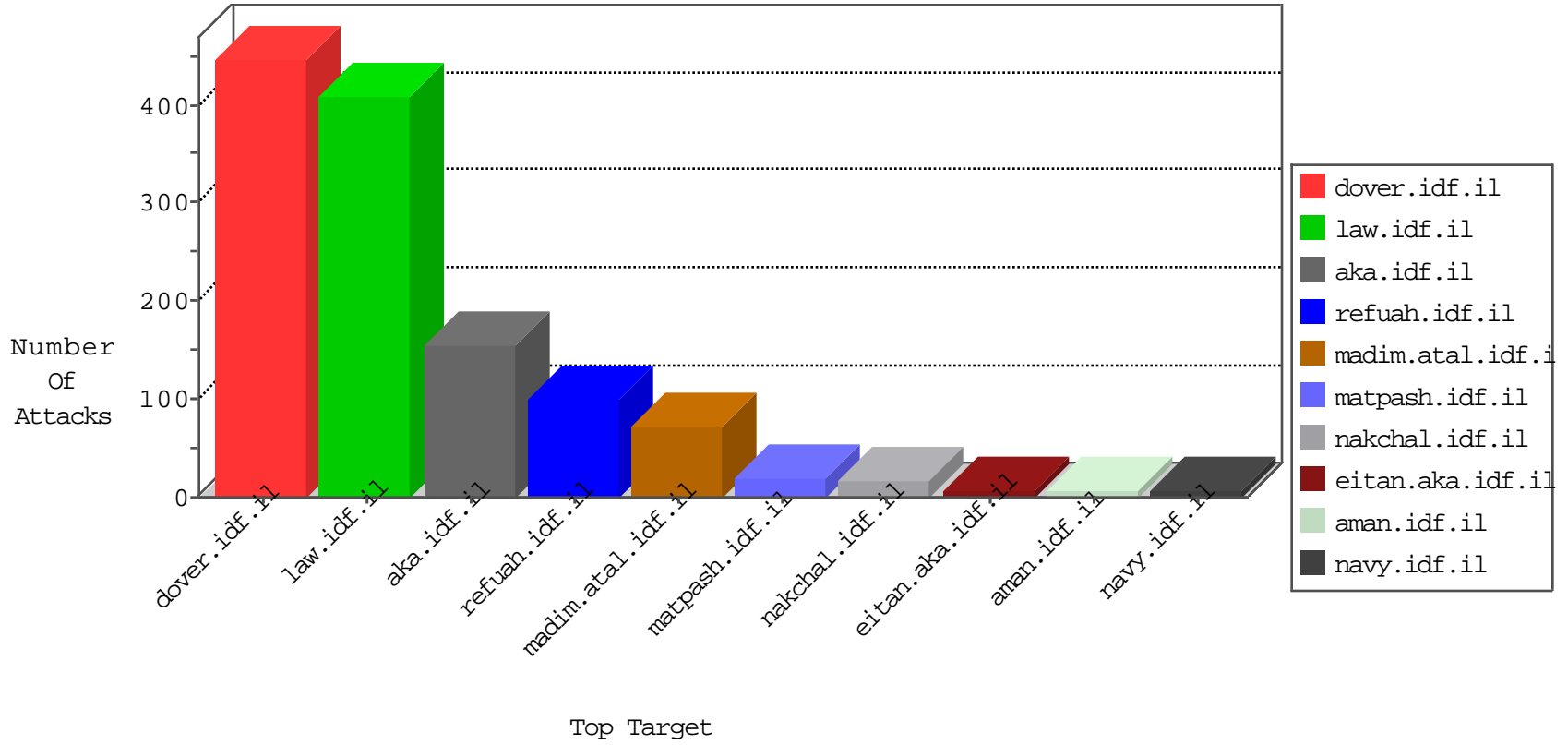


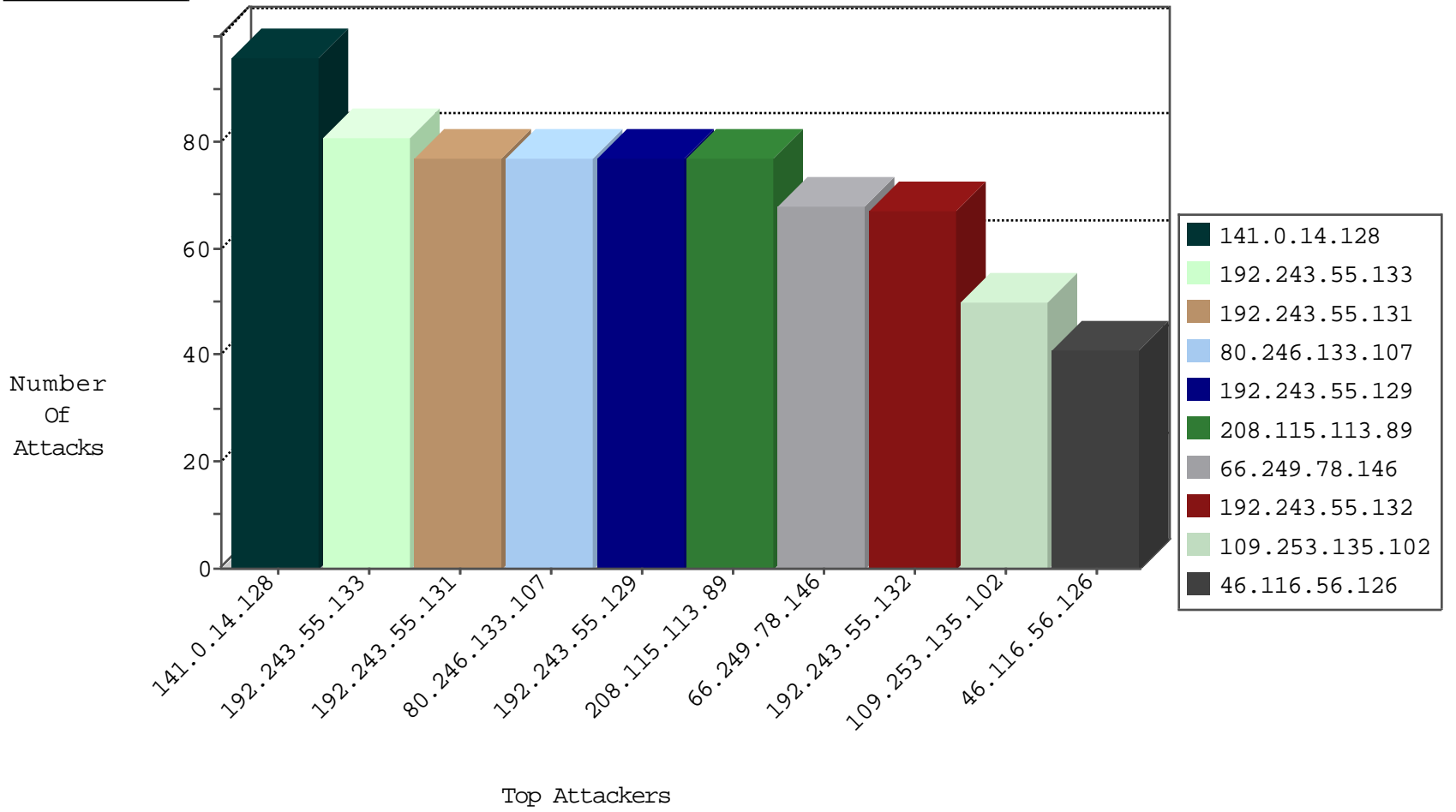
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3231
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	3
79.178.229.60	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
173.208.197.254	United States	147.237.76.30	himush.idf.il	block-sp-trafl	forward	2
173.208.197.251	United States	147.237.76.31	nakchal.idf.il	block-sp-trafl	forward	2
173.208.197.251	United States	147.237.76.42	refuah.idf.il	block-sp-trafl	forward	2
85.25.43.94	Germany	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets_Con_Limit	drop	2
69.30.202.230	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-trafl	drop	1
94.102.52.10	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
5.196.199.231	France	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
69.30.202.226	United States	147.237.77.233	atal.idf.il	block-sp-trafl	drop	1
69.30.202.227	United States	147.237.72.166	aka.idf.il	block-sp-trafl	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
80.246.133.107	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	76
141.0.14.128	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
141.0.14.128	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	29
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	28
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	22
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
172.58.168.198	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
46.116.56.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
46.117.169.121	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	13
109.253.215.252	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	12
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
85.75.79.141	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.116.56.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.129	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.116.56.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.50	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.50	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.116.56.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.135.102	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	50
2.53.22.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
188.143.234.155	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/sendtofriend	Block	4
188.143.232.27	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/sendtofriend	Block	4
185.32.179.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.143.232.27	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.166.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.138.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.199.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.143.234.155	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.177.196.197	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.177.196.197	Block	2
188.143.232.32	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/sendtofriend	Block	2
157.55.39.213	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/iturim/asp/list.asp	Block	1
80.246.133.107	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.234	Block	1
46.120.242.60	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl100\$cphMain\$cphSachar\$ctl109 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.253.215.252	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
208.115.111.71	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list1.htm	Block	1
77.221.69.168	Lithuania	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
2.53.30.164	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 2.53.30.164	Block	1
157.55.39.213	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/brothers/skira/default.asp	None	1
84.228.226.69	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/edim/yoman/yoman.asp	Block	1
187.44.148.42	Brazil	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
54.86.145.194	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
212.76.119.180	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
77.221.69.168	Lithuania	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/edim/yoman/yoman.asp	Block	1
157.55.39.213	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/kamlar/gallery/	None	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/edim/yoman/yoman.asp	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/16838.jpg	Block	1
187.44.148.42	Brazil	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/wp-login.php	Block	1
66.249.64.3	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/yoman.asp	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kapaz/contactus.asp	Block	1
188.143.232.32	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
45.55.196.77	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 45.55.196.77	Block	1
157.55.39.213	United States	147.237.72.166	aka.idf.il	Unknown Parameter pagenum in aka.idf.il/chinuch/gallery/	None	1
207.46.13.14	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12847-he/dover.aspx ; ½, šE f i 7, ç 'f ç, šE f i 7, ç 'f -, šE f "e + 'f "•	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
187.44.148.42	Brazil	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
157.55.39.37	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.177.196.197	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/home/default.aspx	None	1
173.208.197.251	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.qeqe11.com/	Block	1
45.55.196.77	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
207.46.13.75	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/coordinationgaza/officesmap/pages/aza.aspx	Block	1