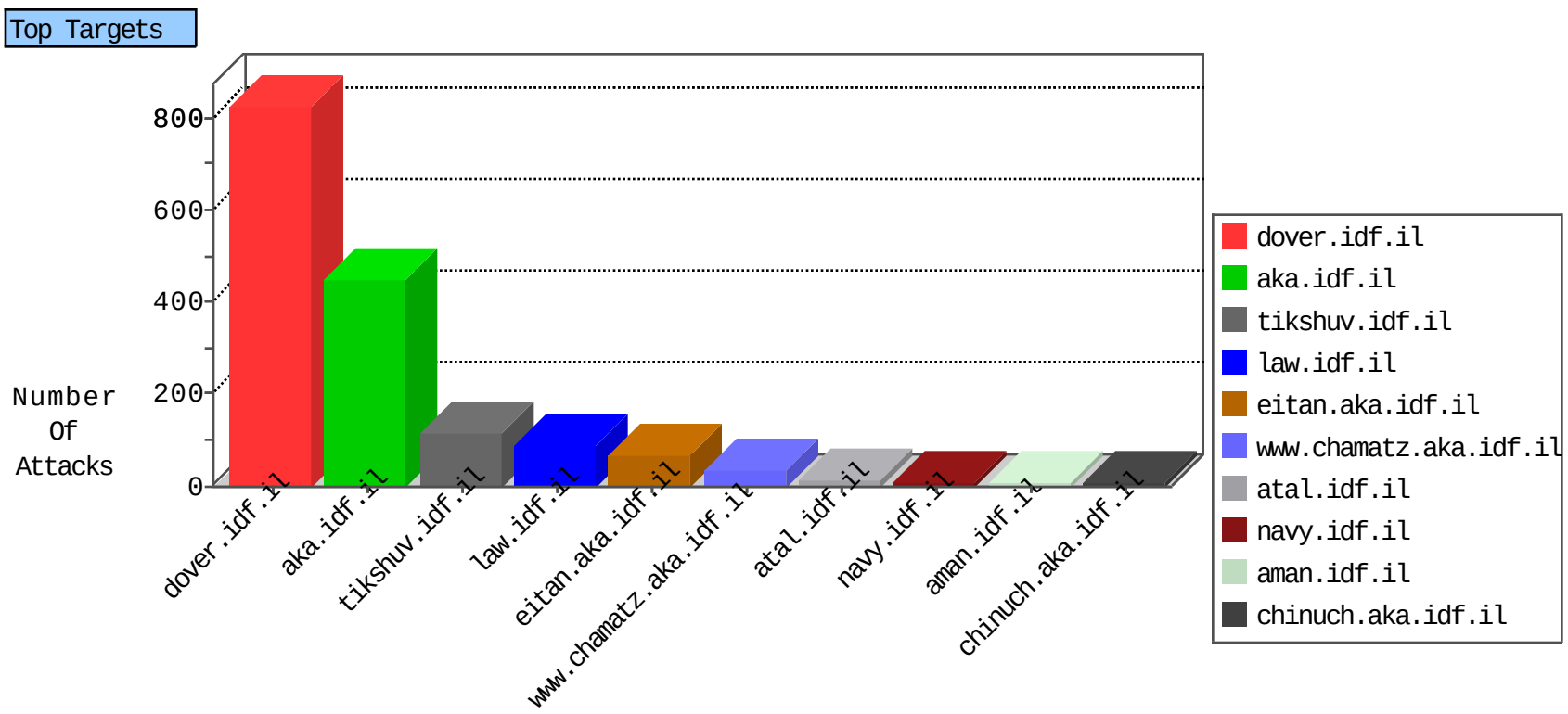
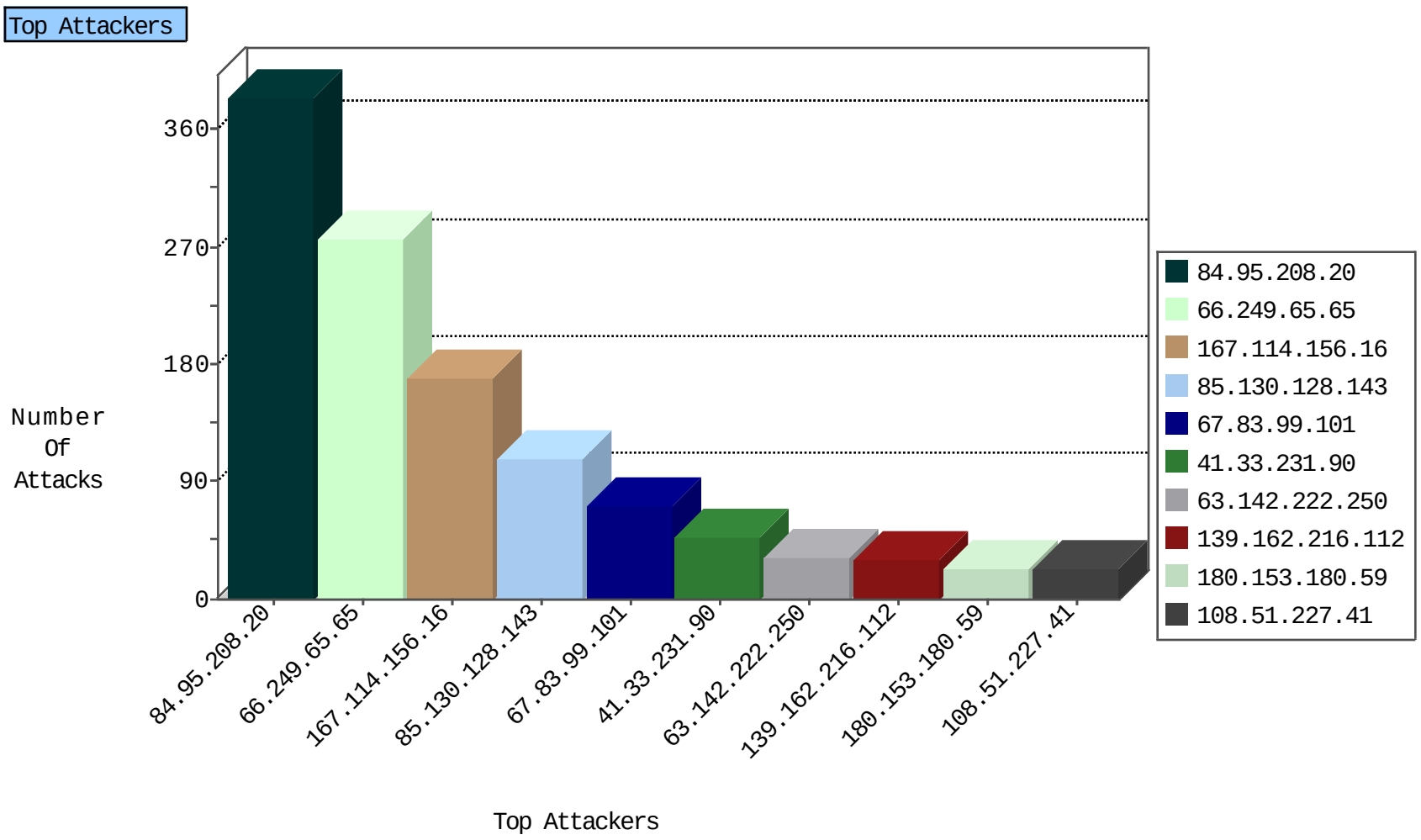
04-22-2016-02:04:05 to 04-22-2016-03:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-22-2016-02:04:05 to 04-22-2016-03:04:05

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	HTTP-POST-Segmented-DoS	dest-reset	7385
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1128
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	9
185.94.111.1	Russian Federation	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

04-22-2016-02:04:05 to 04-22-2016-03:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-22-2016-02:04:05 to 04-22-2016-03:04:05

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
66.249.65.65	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.202	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
91.201.236.158	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
84.200.15.174	147.237.8.14	Germany	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
84.200.15.174	147.237.8.14	Germany	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
81.169.171.4	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
58.218.211.11	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
183.3.202.115	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
87.79.42.120	147.237.77.179	Germany	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
84.200.15.174	147.237.8.14	Germany	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
81.169.171.4	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
66.249.65.65	147.237.72.166	United States	aka.idf.il	WEB-CGI redirect access	1

04-22-2016-02:04:05 to 04-22-2016-03:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	264
67.83.99.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
85.130.128.143	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
85.130.128.143	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	32
85.130.128.143	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	31
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
63.142.222.250	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
180.153.180.59	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
108.51.227.41	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.65.21	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
101.227.59.225	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.126.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
180.153.180.58	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.179.9.36	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
85.130.231.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
180.153.180.85	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.130.231.236	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.73.243	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
185.32.179.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
63.142.222.250	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
207.46.13.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.129	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	4
173.66.153.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.64.41	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.130.128.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	118
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	72
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	25
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	12
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	10
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.65.65	Block	7
149.202.239.135	France	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter PageNum	Block	6
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	4
149.202.239.134	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
17.138.55.96	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21229-he/idfgdover.aspx	Block	2
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
157.55.39.15	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.231.43	Block	1
54.210.18.124	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
82.80.150.191	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
192.243.55.135	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcdhphdmltxdewmtguzg9j&infocenteritem=true	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/shalishut/site/gallery.aspx	None	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
157.55.39.95	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nahal	Block	1
66.249.64.41	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
149.202.239.134	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId\u003d58624 in www.aka.idf.il/main/giyus/general.aspx	None	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
157.55.39.139	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
79.177.232.146	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 79.177.232.146	Block	1
66.249.64.119	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
79.177.232.146	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/mobile	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
149.202.239.135	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	1
54.210.18.124	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
79.180.245.250	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
95.86.77.216	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1