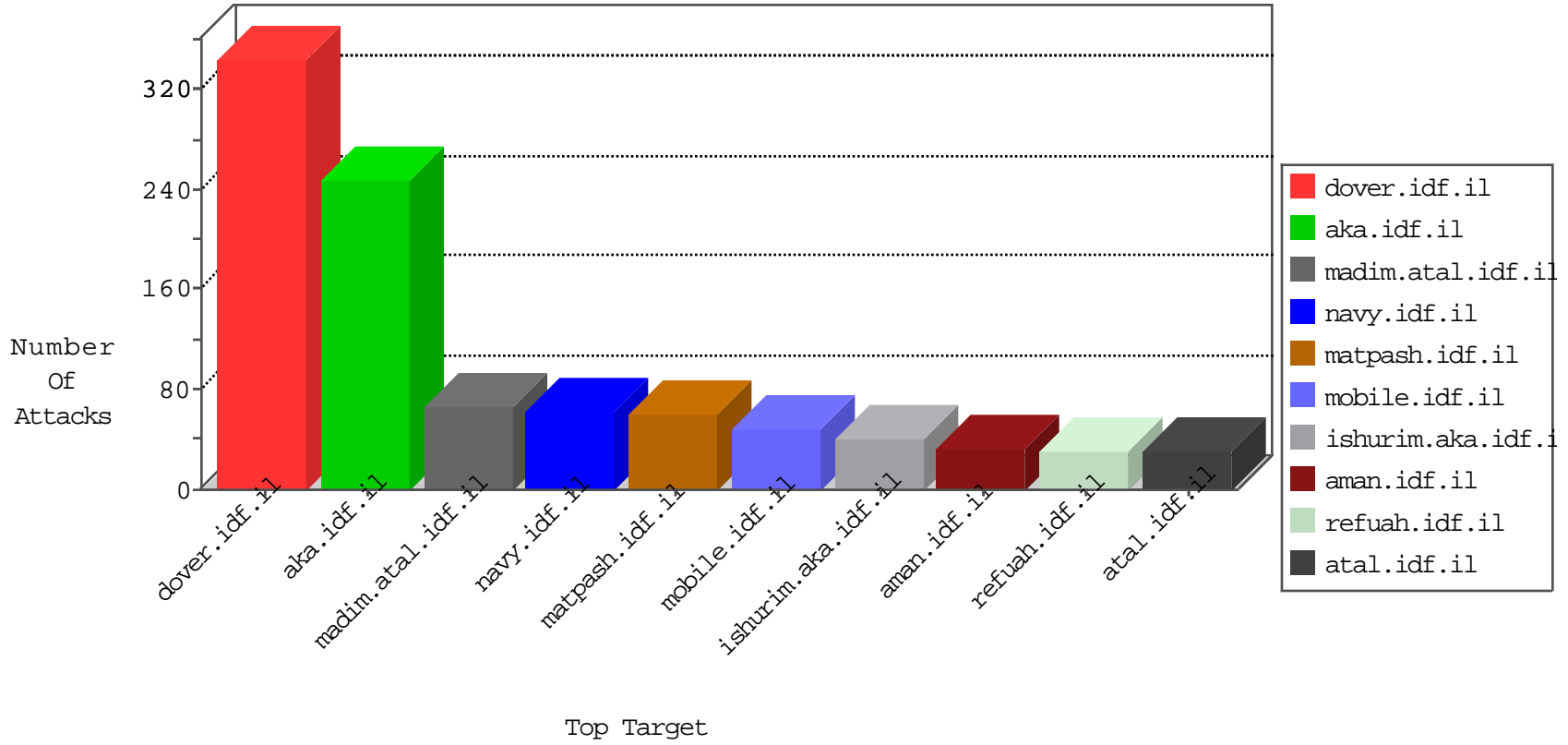


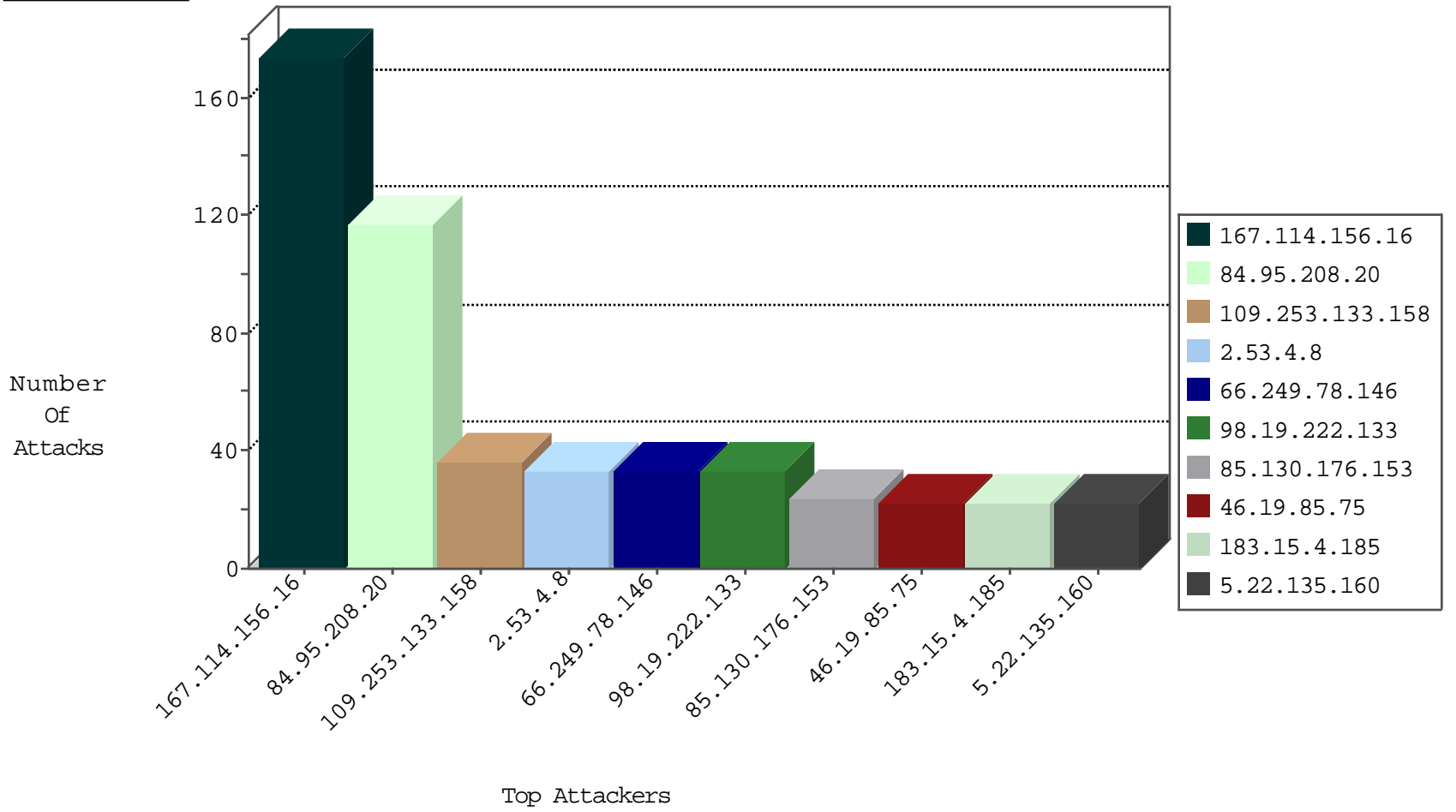
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	8746
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6666
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2818
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	45
59.57.245.40	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	8
60.173.56.71	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
178.57.124.52	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
46.19.86.48	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
118.125.89.119	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.219.122.4	Poland	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
98.19.222.133	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
74.63.228.226	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3
98.19.222.133	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
195.74.38.14	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
98.19.222.133	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	26
91.219.122.4	147.237.77.176	Poland	matpash.idf.il	SQL Injection - Select From	8
195.74.38.14	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	6
74.63.228.226	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	4
134.191.232.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.206.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.164.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
23.96.109.87	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 4096	1
176.13.22.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.192.204.41	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	147.237.77.233	Italy	atal.idf.il	ET SCAN NMAP -f -sS	1
109.253.192.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.109.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
220.249.194.151	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
31.210.187.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
13.92.178.142	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.12.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	147.237.77.233	Italy	atal.idf.il	ET SCAN NMAP -sS window 2048	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
5.22.135.160	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
2.53.4.8	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.142.68.16	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
2.55.165.129	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
176.13.21.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.18.195	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
162.243.118.199	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.35	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
183.15.4.185	China	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
213.14.44.2	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.130.176.153	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.130.176.153	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
213.14.44.2	Turkey	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
85.130.176.153	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
109.253.216.233	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.178.159.148	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
109.65.201.253	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.74.105.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	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
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.117.105.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.110.183.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.55.184.111	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.176.56.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.50	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.142.201.160	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.182.29.211	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.50	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.53.36.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.145.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.19.75	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.47.240	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.155.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.42	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.209.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.214.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.1.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.176.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-20-2016-09:04:09 to 04-20-2016-10:04:09

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.184	Europe	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
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	42
109.253.133.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
2.53.4.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
176.13.13.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
2.53.175.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
176.13.21.242	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	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	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
46.117.157.81	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.117.157.81	Block	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
176.13.12.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	2
109.226.45.55	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
40.77.167.54	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
79.182.43.124	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	2
36.79.196.19	Indonesia	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
66.249.75.118	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.118	Block	2
36.79.196.19	Indonesia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	2
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.83	Israel	147.237.76.31	nakchal.idf.il	Distributed Illegal HTTP Version	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
5.39.222.159	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/rom-0	Block	1
192.117.105.2	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteriten/	Block	1
82.81.101.124	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
109.253.211.226	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
46.117.157.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	1
37.9.122.203	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16364-	Block	1
2.53.4.8	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
183.15.4.185	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 183.15.4.185	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1815-he/dover.aspx	Block	1
141.212.122.161	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
46.19.85.83	Israel	147.237.76.31	nakchal.idf.il	Distributed Malformed URL	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	1
207.46.13.39	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/links.aspx	Block	1
110.89.60.108	China	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
62.210.254.52	France	147.237.72.166	aka.idf.il	Unknown Parameter amp/w in www.aka.idf.il/main/giyus/captcha.ashx	None	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	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
2.53.156.76	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
183.15.4.185	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
79.181.19.90	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.aspx/getauthuser	Block	1
157.55.39.219	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/g/yus	Block	1