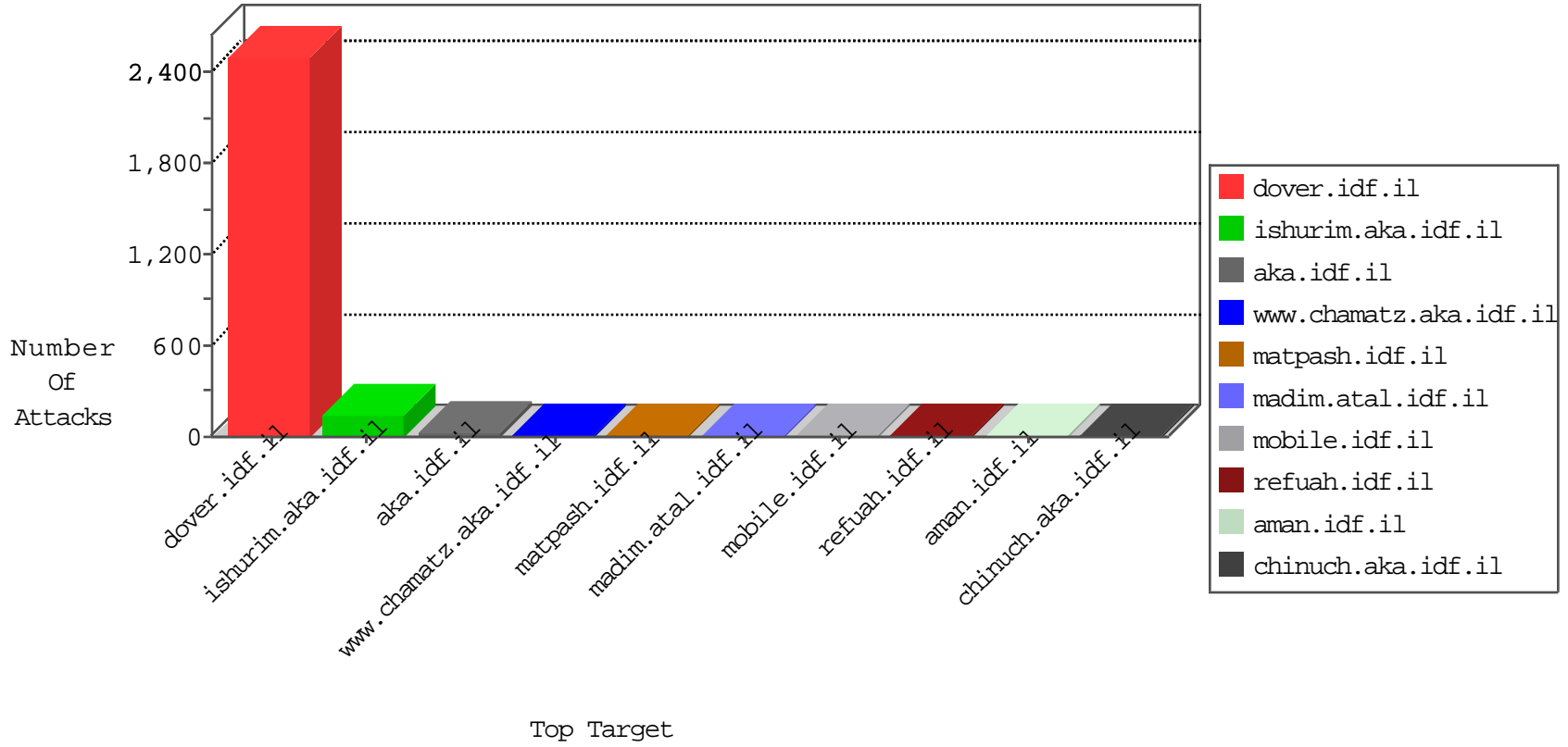


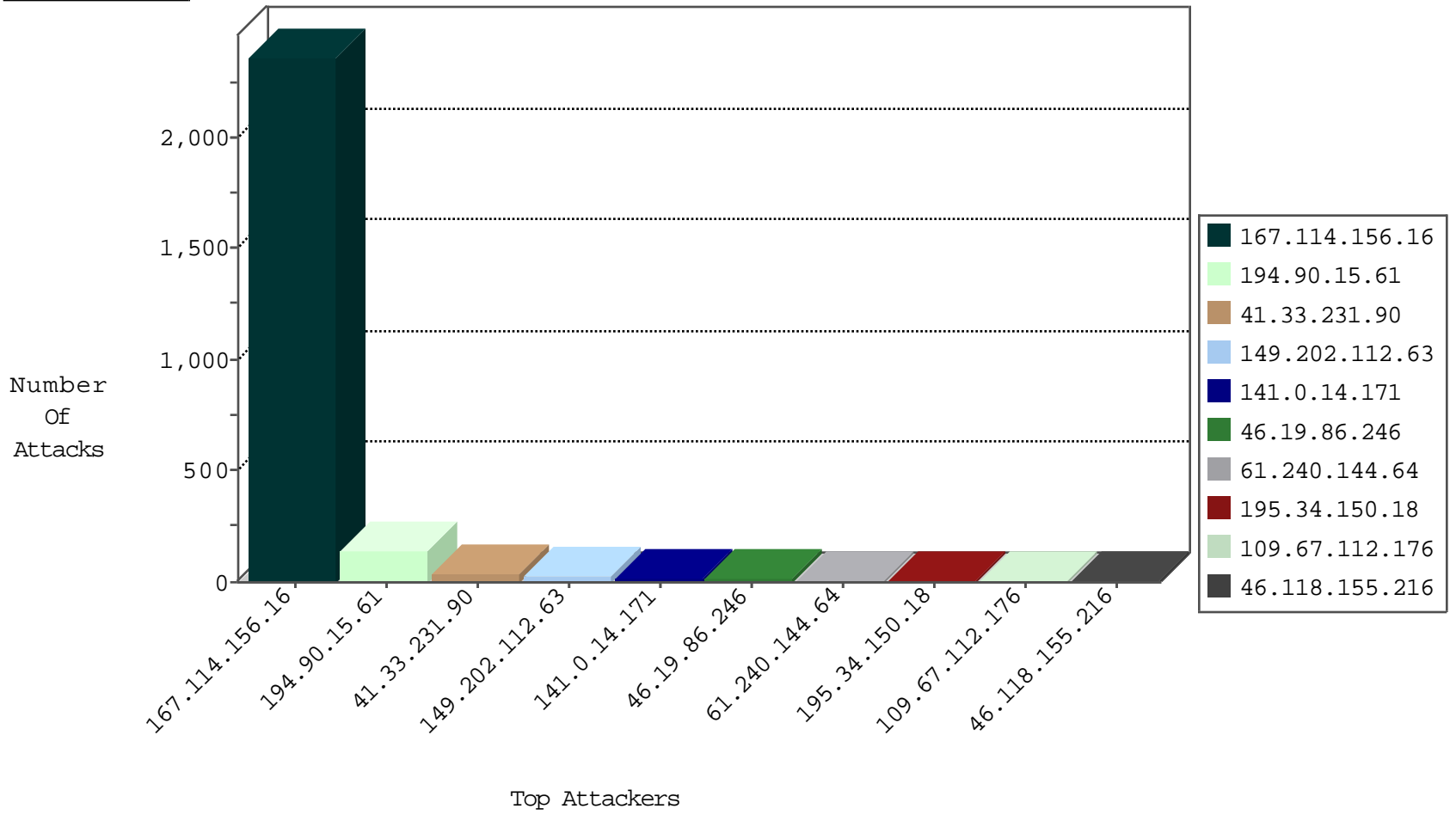
IDF Under Attack Daily Report



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	DOS-Tool-SwitchbladG	dest-reset	3401
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	896
115.239.228.10	China	147.237.0.34	tikshuv.idf.il	Frk_Under_Attack_Con_Http	drop	2
115.239.228.10	China	147.237.0.34	tikshuv.idf.il	Frk_Purple_Con_Limit_Http	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.202.112.63	Germany	147.237.77.216	dover.idf.i	0361: HTTP: Protected File Access (/etc/passwd)	Block	1
149.202.112.63	Germany	147.237.77.216	dover.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
149.202.112.63	Germany	147.237.77.216	dover.idf.i	2809: HTTP: IIS TRACK Method	Block	1
149.202.112.63	Germany	147.237.77.216	dover.idf.i	3886: HTTP: Cross Site Scripting in POST Request	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
61.240.144.64	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.42	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.198	China	e.yochanan.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.77.243	United States	mobile.idf.il	ET DROP Dshield Block Listed Source	1
61.240.144.64	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
149.202.112.63	147.237.77.216	Germany	dover.idf.il	GPL WEB_SERVER TRACE attempt	1
37.143.82.50	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
109.228.33.167	147.237.72.217	United Kingdom	e.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.60.89	147.237.0.16	Netherlands	my-kosher-kraivi.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.72.14	Ukraine	dover.idf.il(old)	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.240.144.64	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.42	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.42	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
149.202.112.63	147.237.77.216	Germany	dover.idf.il	SERVER-WEBAPP TRACE attempt	1
61.240.144.64	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
149.202.112.63	147.237.77.216	Germany	dover.idf.il	GPL WEB_SERVER /etc/passwd	1
37.143.82.50	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.60.89	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
79.129.125.192	147.237.0.19	Greece	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
141.0.14.171	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
46.19.86.246	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.180.134.215	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.246	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.11	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.202.112.63	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
213.57.145.90	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
85.250.255.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
109.67.112.176	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
213.57.145.90	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
54.241.198.78	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
184.105.139.119	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
184.105.247.227	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.130.78.65	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
74.82.47.20	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.79.168.168		147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.247.199	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.202.112.63	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
187.137.36.112	Mexico	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
23.29.122.222	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
174.236.36.41	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.48	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.199	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
154.127.64.35	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
89.248.167.162	Netherlands	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
23.96.208.137	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.91	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.70	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.207	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
155.94.222.12	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
89.248.167.162	Netherlands	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
73.49.31.119	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.170	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.119	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
216.218.206.106	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.208	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
89.248.167.162	Netherlands	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
74.82.47.10	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.172	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.90.15.61	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 194.90.15.61	Block	142
149.202.112.63	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 149.202.112.63	Block	8
109.67.112.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	4
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
149.202.112.63	Germany	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 149.202.112.63	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
40.77.167.89	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/headerupper/	Block	1
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Unknown Parameter l in www.chinuch.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
73.49.31.119	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
149.202.112.63	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
216.218.206.66	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
184.168.152.148	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/wp-admin/	Block	1
141.0.14.171	Europe	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
81.209.177.95	Europe	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/shared/usercontrols/headerupper/	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
149.202.112.63	Germany	147.237.77.216	dover.idf.il	Unknown HTTP Request Method NETSPARKER in URL www.idf.il/894-he/dover.aspx	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
219.94.129.86	Japan	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/old/wp-admin/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
184.168.200.23	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/wp/wp-admin/	Block	1
82.145.45.44	United Kingdom	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17900-en/dover.aspxyou	Block	1
157.55.39.113	United States	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
187.137.36.112	Mexico	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
85.250.255.44	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
157.55.39.113	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8814-he/counter2812009124353/counter.php	Block	1
109.66.37.137	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
72.29.127.17	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/blog/wp-admin/	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19538-he/dover.aspx	Block	1
194.90.15.61	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many 404: Response Code per Session	Block	1
149.202.112.63	Germany	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
212.1.210.166	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/test/wp-admin/	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1356-he/refuah.aspx	Block	1