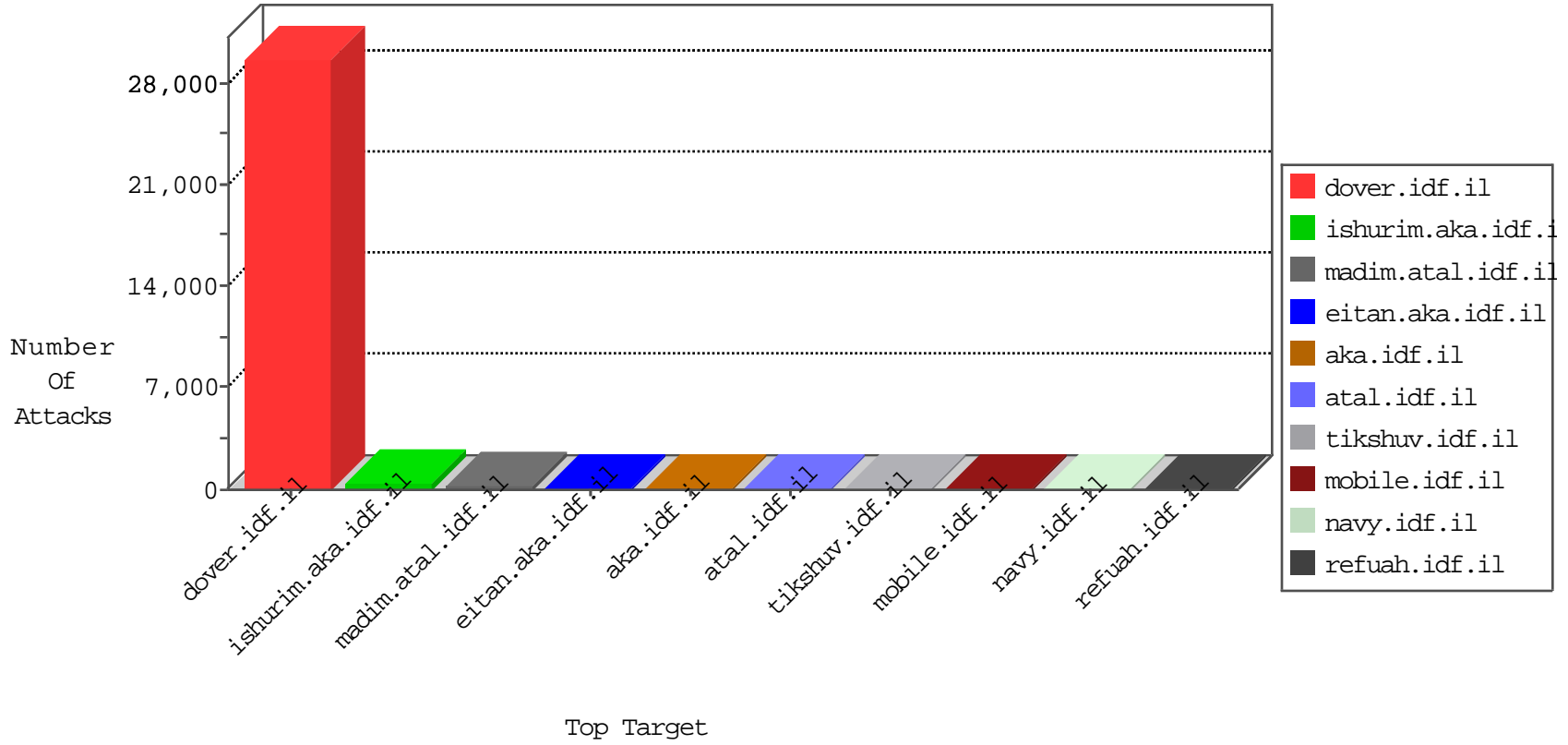




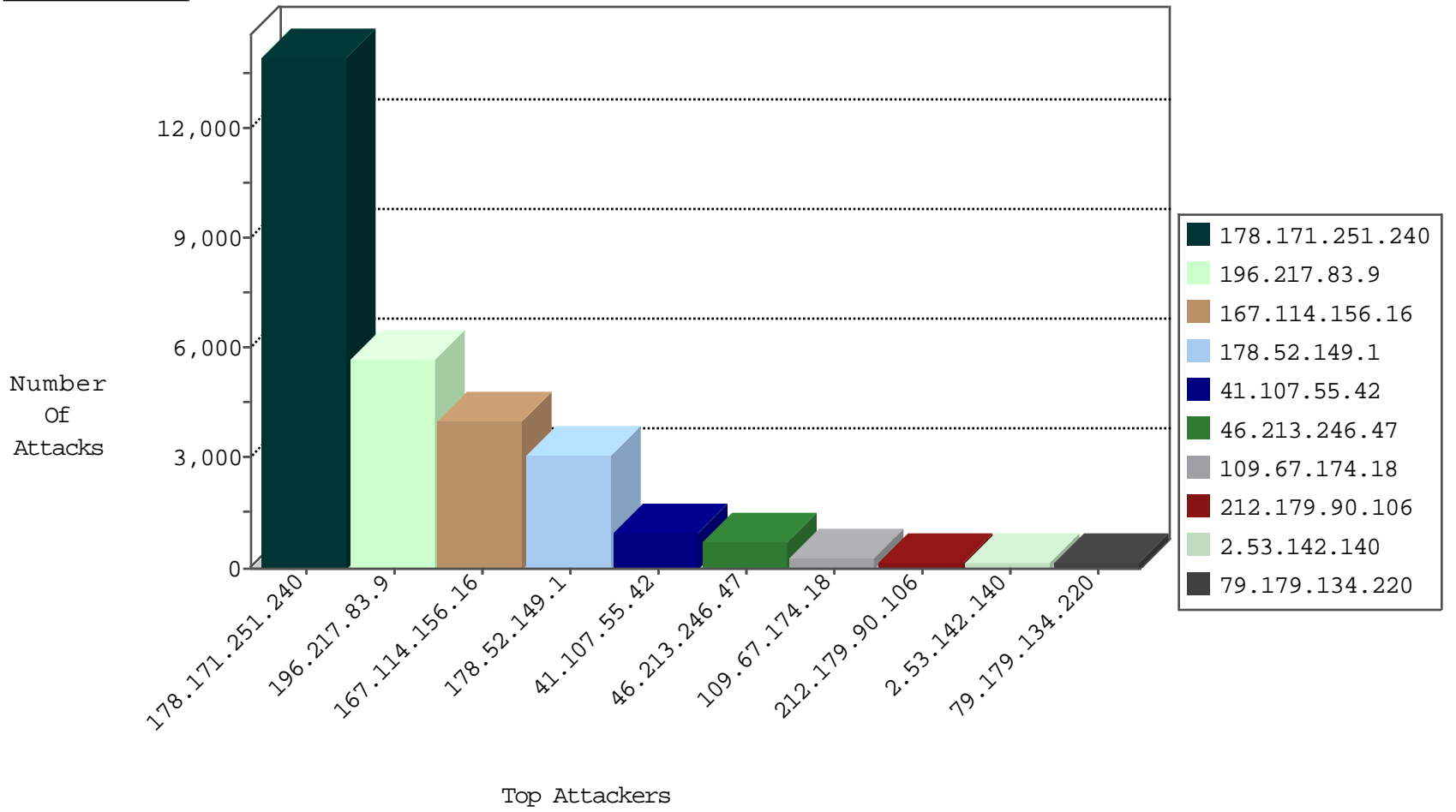
# IDF Under Attack Daily Report



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	Block_Ip_Web_In	drop	3989
41.107.55.42	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	991
196.217.83.9	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	361
173.3.228.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
196.218.61.220	Egypt	147.237.0.34	tikshuv.idf.il	L4 Source or Dest Port Zero	drop	6
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
123.59.59.52	China	147.237.0.19	madim.atal.idf.il	block-sp-trafl	forward	2
134.147.203.115	Germany	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
134.147.203.115	Germany	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	2
101.201.147.32	China	147.237.77.233	atal.idf.il	block-sp-trafl	forward	2
185.94.111.1	Russian Federation	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
200.160.6.137	Brazil	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
188.138.17.205	France	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
179.43.141.194	Switzerland	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
85.64.0.183	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.135.131	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
179.43.141.194	Switzerland	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
79.181.117.197	Israel	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.20.22	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
94.159.166.130	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.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
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

## 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	10
80.246.130.65	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
185.112.248.50	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
185.112.248.50	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
106.186.113.132	147.237.77.176	Japan	matpash.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
91.201.236.158	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.158	147.237.76.201	Ukraine	e.atal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
185.112.248.50	147.237.72.217	United Kingdom	e.idf.il	ET SCAN Potential SSH Scan	1
185.112.248.50	147.237.8.27	United Kingdom	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
115.178.27.90	147.237.0.33	Cambodia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.158	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.158	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN NMAP -f -sS	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	6942
196.217.83.9	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5146
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3610
178.52.149.1	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3063
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2637
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	626
46.213.246.47	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	586
109.67.174.18	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	300
196.217.83.9	Morocco	147.237.77.216	dover.idf.il	drop		drop	187
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	155
79.179.134.220	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	129
159.203.100.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
128.69.170.170	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
46.213.246.47	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	49
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	45
54.162.16.100	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
46.213.246.47	Syrian Arab Republic	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	41
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
46.213.246.47	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
17.142.152.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
17.142.156.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
17.142.152.72	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
17.142.152.111	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
85.64.0.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
178.52.149.1	Syrian Arab Republic	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	23
46.213.246.47	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
79.176.30.186	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
79.176.30.186	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
79.180.168.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	16
46.19.86.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
174.22.244.151	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
178.171.251.240	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
5.28.145.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
85.64.1.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
99.59.222.193	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
178.52.149.1	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
17.142.145.3	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.28.190.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
17.142.152.68	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.213.246.47	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack		reject	8
80.246.130.65	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
93.173.233.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
178.52.149.1	Syrian Arab Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.142.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	153
2.53.49.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
213.57.183.218	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 213.57.183.218	Block	6
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	4
213.57.183.218	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	3
46.117.181.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.215	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
159.203.100.118	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 159.203.100.118	Block	2
159.203.100.118	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22929-ar/idfgdover.aspx	Block	1
109.64.98.133	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus_	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
207.46.13.172	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/undefined	Block	1
149.50.24.121	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 149.50.24.121	Block	1
77.237.146.28	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
46.19.85.241	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
197.167.4.145	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
109.67.34.235	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
23.101.61.176	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-23118-he/dover.aspx/	Block	1
157.55.39.81	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
91.79.240.239	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
2.53.156.226	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
198.179.71.70	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/templates/links/mobile	Block	1
130.185.155.10	Sweden	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3269.jpg	Block	1
27.159.234.88	China	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
157.55.39.106	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
106.186.113.132	Japan	147.237.76.31	nakchal.idf.il	Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.23	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1
2.53.171.228	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/templates/general/mobile	Block	1
130.185.155.10	Sweden	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/wp-login.php	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2372.jpg	Block	1
106.186.113.132	Japan	147.237.77.176	matpash.idf.il	Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.82	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.82	Block	1
2.53.191.238	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/links/mobile	Block	1
149.50.24.121	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
40.77.167.18	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1