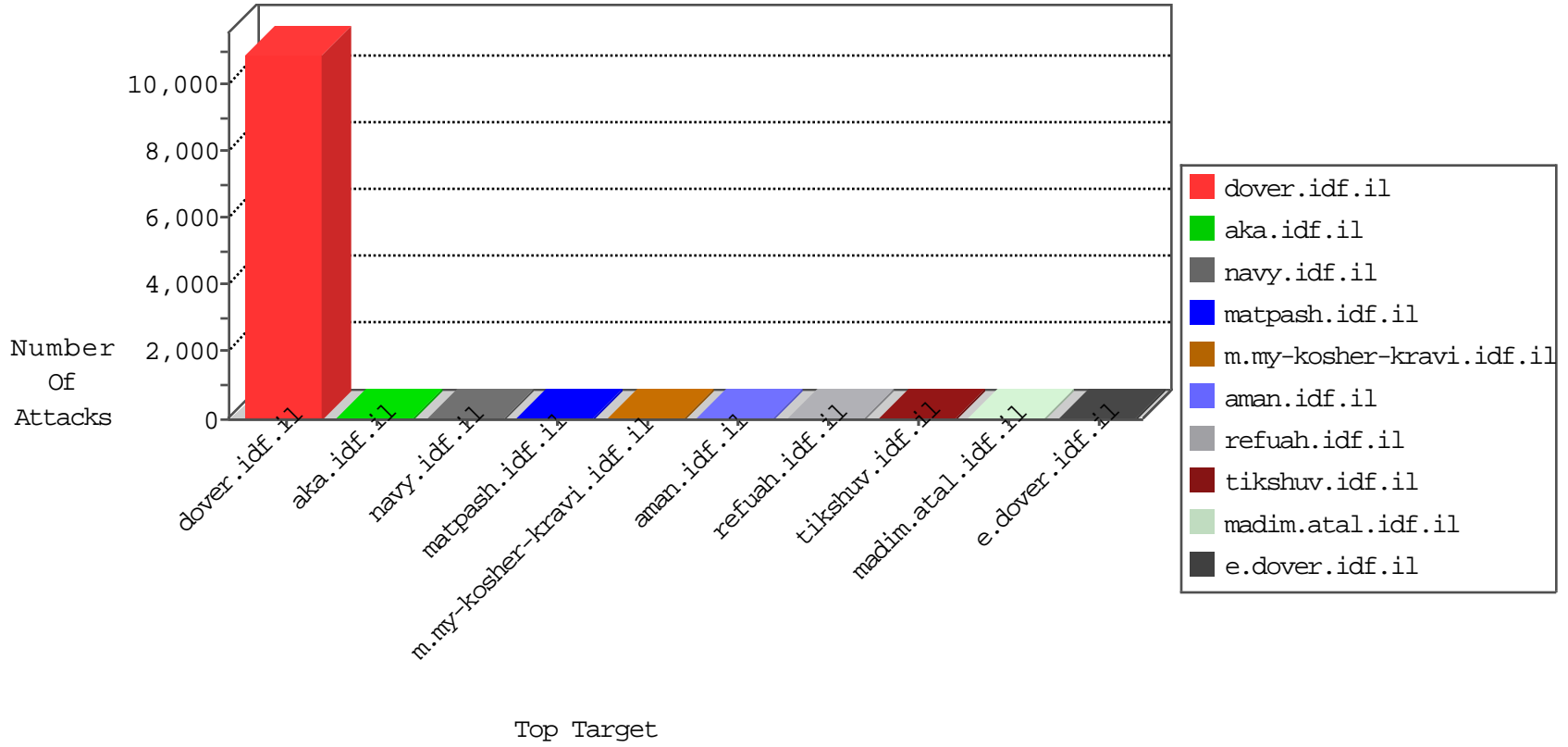




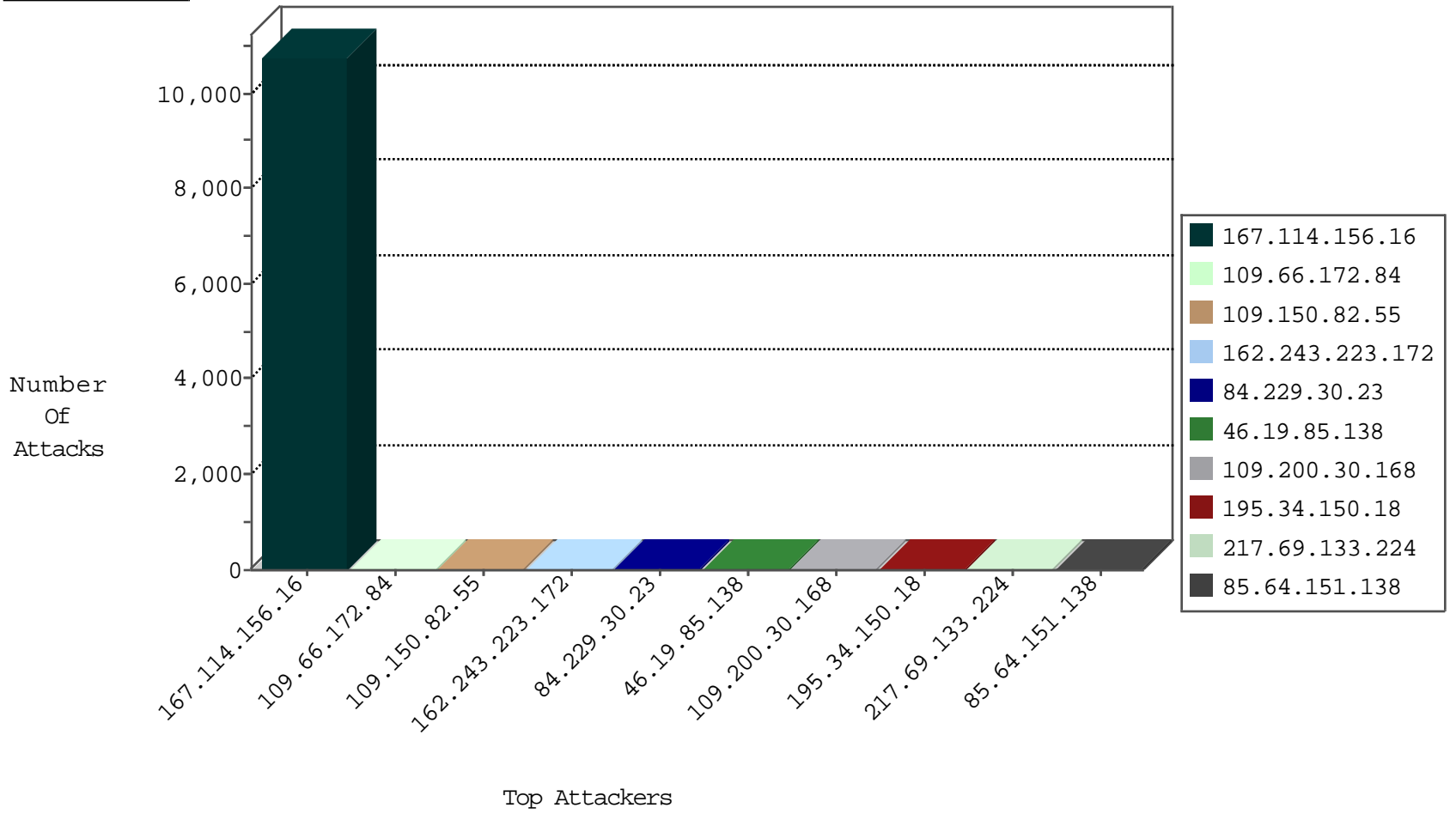
# IDF Under Attack Daily Report



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	1525
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.150.82.55	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
157.55.39.166	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
212.179.54.237	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	F_Dover_Under_Attack_Con_Http	drop	3
173.208.137.10	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
180.97.106.37	China	147.237.77.74	law.idf.il	block-sp-trafl	drop	1
180.97.106.36	China	147.237.76.39	mobile.meitav.idf.il	block-sp-trafl	drop	1
180.97.106.161	China	147.237.77.234	halag.idf.il	block-sp-trafl	drop	1
180.97.106.36	China	147.237.77.233	atal.idf.il	block-sp-trafl	drop	1
180.97.106.162	China	147.237.0.15	kosher-kravi.idf.il	block-sp-trafl	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
180.97.106.37	China	147.237.0.34	tikshuv.idf.il	block-sp-trafl	drop	1
146.185.239.100	Russian Federation	147.237.77.235	sviva.idf.il	block-sp-trafl	drop	1
180.97.106.162	China	147.237.77.19	law-forum.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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
208.67.1.25	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.162	147.237.72.156	China	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.161	147.237.8.45	China	e.eitan.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.37	147.237.0.34	China	tikshuv.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.36	147.237.0.19	China	madim.atal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
149.71.157.125	147.237.8.28	Italy	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
149.71.157.125	147.237.0.19	Italy	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.25	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.161	147.237.76.86	China	navy.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.37	147.237.76.31	China	nakchal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.36	147.237.76.176	China	test.ncore.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
149.71.157.125	147.237.8.46	Italy	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
149.71.157.125	147.237.0.34	Italy	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
149.71.157.125	147.237.0.15	Italy	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9700
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1000
109.66.172.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
162.243.223.172	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
84.229.30.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
217.69.133.224	Russian Federation	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.172.84	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
109.150.82.55	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.150.82.55	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
109.150.82.55	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
72.106.70.55	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.142.52.154	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
212.35.64.194	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
37.247.36.78	Netherlands	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
192.114.91.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.153.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.18	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
217.69.133.223	Russian Federation	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
66.249.78.153	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.111.72	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
74.82.47.36	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.86	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.115	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.111.120.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.219	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.121.214.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
146.185.239.102	Russian Federation	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
27.46.137.27	China	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
104.128.144.131	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.89.24.53	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.92	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.120	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.121.214.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.146.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
112.135.68.33	Sri Lanka	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
108.61.123.88	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.104	United States	147.237.0.35	akaws.idf.il	drop		drop	1
74.89.24.53	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.93	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.65.232.169	Israel	147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
157.55.39.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
37.26.147.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6
213.251.182.114	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.251.182.114	Block	4
162.243.223.172	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 162.243.223.172	Block	4
85.64.151.138	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	4
85.64.151.138	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 85.64.151.138	Block	3
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	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
23.254.138.210	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
195.154.127.146	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
157.55.39.76	United States	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
180.97.106.37	China	147.237.76.31	nakchal.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	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
72.47.224.35	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
38.111.147.84	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
217.69.133.225	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-12321-en	Block	1
180.97.106.161	China	147.237.76.86	navy.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.201.154.207	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.181.169.197	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
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	1
162.243.223.172	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
103.9.170.141	Australia	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ the idf official website	Block	1
2.54.158.151	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding B4hnUU&AZ7B-g&P%PA\$XPYrv in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
180.97.106.162	China	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
151.236.51.108	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
83.243.58.157	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
65.55.210.120	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
180.97.106.36	China	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
2.54.158.151	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 2.54.158.151	None	1
184.105.247.195	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.69	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
84.191.27.126	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.65.25	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/110571.pdf	Block	1
180.97.106.37	China	147.237.0.34	tikshuv.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1