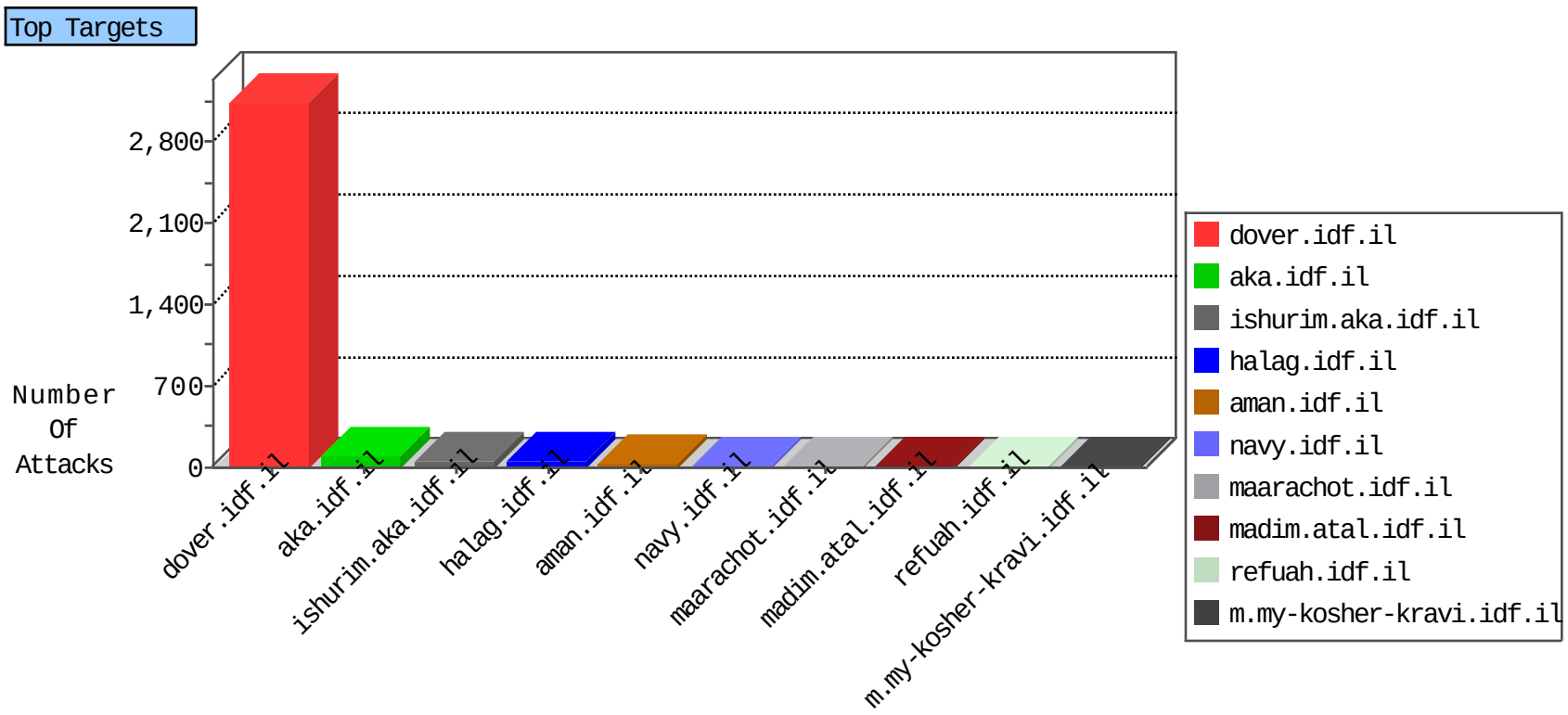
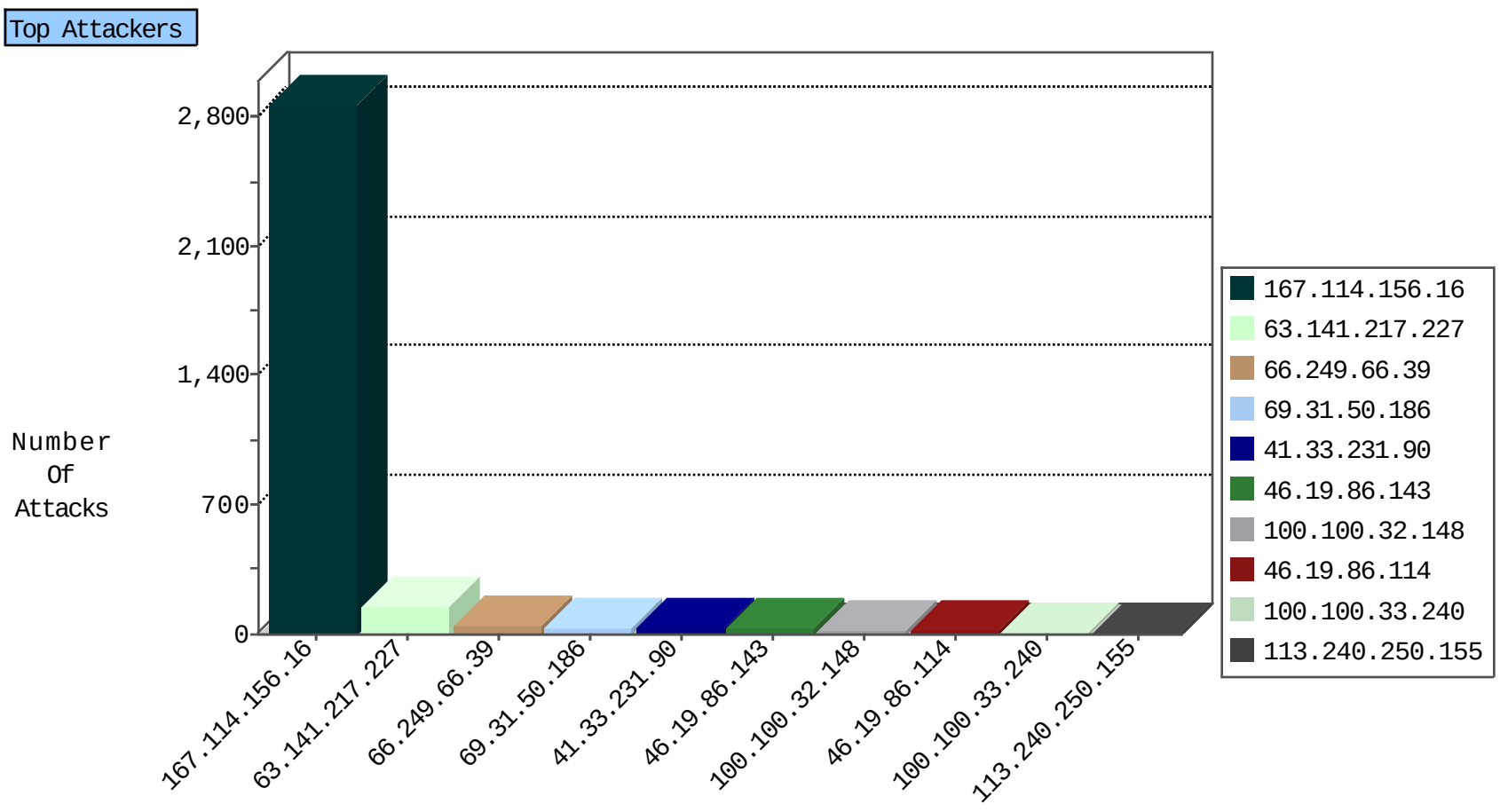
12-04-2015-07:04:03 to 12-04-2015-08:04:03

IDF Under Attack Daily Report



Top Target



Top Attackers

12-04-2015-07:04:03 to 12-04-2015-08:04:03

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	3588
66.249.64.50	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	754
69.31.50.186	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
95.154.64.37	Russian Federation	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	3
192.3.170.124	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.36	China	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.36	China	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
192.3.170.124	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

12-04-2015-07:04:03 to 12-04-2015-08:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-04-2015-07:04:03 to 12-04-2015-08:04:03

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	5
113.240.250.155	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.155	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
85.17.156.69	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
62.38.250.31	147.237.72.156	Greece	aman.idf.il	ET SCAN NMAP -sS window 3072	1
222.186.56.32	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
23.92.209.204	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
200.35.150.97	147.237.77.178	Panama	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
23.92.209.204	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
116.121.137.5	147.237.77.178	Korea, Republic of	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
113.240.250.155	147.237.8.46	China	e.chinuch.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
113.240.250.155	147.237.0.17	China	m.my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
85.17.156.69	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
65.255.43.24	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
222.186.56.32	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.166.188.68	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
200.35.150.97	147.237.77.178	Panama	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
23.92.209.204	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
200.35.150.97	147.237.77.176	Panama	matpash.idf.il	ET SCAN Potential SSH Scan	1
23.92.209.204	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
116.121.137.5	147.237.77.178	Korea, Republic of	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
116.121.137.5	147.237.77.178	Korea, Republic of	e.matpash.idf.il	ET SCAN NMAP -f -sS	1

12-04-2015-07:04:03 to 12-04-2015-08:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
63.141.217.227	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	144
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.86.143	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
100.100.32.148		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	23
46.19.86.114	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
100.100.33.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
69.31.50.186	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.66.42	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.75.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
77.125.116.55	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.115	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
69.31.50.186	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.177.171.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.16	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.117.140.158	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.62.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.62.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.215.168	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.129.179.57	Belgium	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
77.127.85.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.17.190	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.249.64.198	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.68.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.108.17.190	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
70.39.186.218	Satellite Provid	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	3
79.178.125.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.145.95.43	United Kingdom	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.29.192.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.81.209	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
31.210.186.129	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
95.35.181.66	Israel	147.237.77.212	e.dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.66.45	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
8.37.227.70	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
5.102.254.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
113.240.250.155	China	147.237.0.17	m.my-kosher-kravi.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	2
213.57.138.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.75.110	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
41.131.100.197	Egypt	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	2
70.39.186.222	Satellite Provid	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
113.240.250.155	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.175.183.170	Lebanon	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
85.17.156.69	Netherlands	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
196.41.122.249	South Africa	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	3
199.16.156.125	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/1/size220x0/11591.jpg	Block	3
41.78.6.166	South Africa	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	3
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	2
46.19.85.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.3.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
41.78.6.166	South Africa	147.237.77.170	maarachot.idf.il	Distributed Admin Blocking	Block	2
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.75	Block	2
199.59.148.211	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/1/size220x0/11591.jpg	Block	2
196.41.122.249	South Africa	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/index.php	Block	2
41.78.6.166	South Africa	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/index.php	Block	2
199.16.156.124	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/1/size220x0/11591.jpg	Block	2
31.31.196.39	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.78	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/rabanut/general.aspx	Block	1
66.249.66.23	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1133-ar/hamaz.aspx	Block	1
113.240.250.155	China	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_SERVER_HELLO)	None	1
216.218.206.66	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
79.181.104.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
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
66.249.75.110	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	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
196.41.122.249	South Africa	147.237.77.170	maarachot.idf.il	Multiple Admin Blocking from 196.41.122.249	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/an..	Block	1
157.55.39.106	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
46.19.85.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.230.168	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1
199.30.24.57	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1613-15489-he/dover.aspx	Block	1
185.3.146.91	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	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
69.65.3.245	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	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
196.41.122.249	South Africa	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 196.41.122.249	Block	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1074-he/atal.aspx	Block	1
157.55.39.196	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/forgotpassword.aspx	Block	1
66.249.64.74	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/m/	Block	1
93.172.143.100	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/112901.pdf	Block	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/giyus/general.aspx	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-15867-en/dover.aspx	Block	1
188.40.0.147	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
109.65.171.196	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
41.78.6.166	South Africa	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 41.78.6.166	Block	1
72.229.130.220	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
209.68.5.114	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
66.249.66.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/www.youtube.com/v/qgwd7-4a5_m	Block	1
157.55.39.196	United States	147.237.72.166	aka.idf.il	Unknown Parameter 1225bd80 in www.aka.idf.il/iturim/asp/results.asp	None	1
66.249.64.166	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/938-he/nakhal.aspx	Block	1