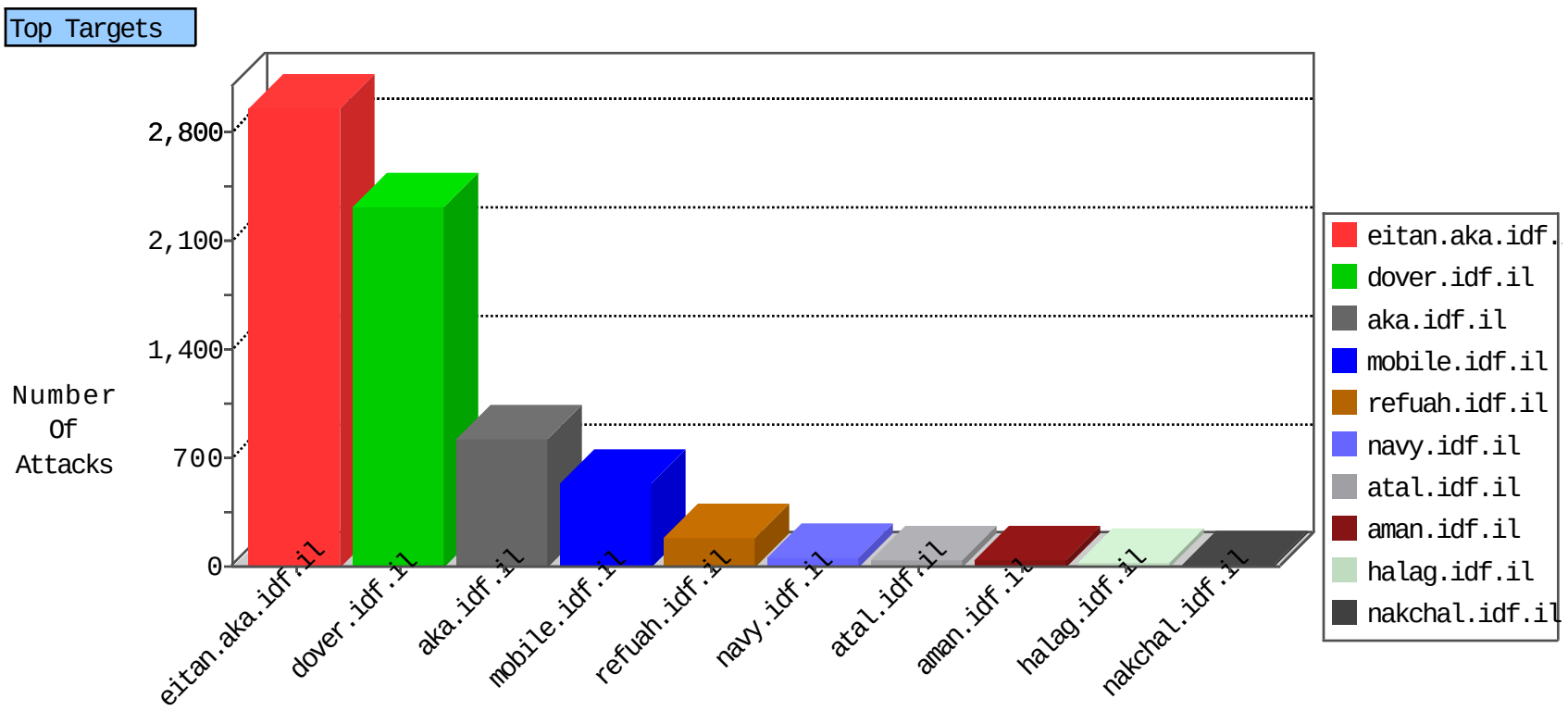
10-31-2015-15:04:08 to 10-31-2015-16:04:08

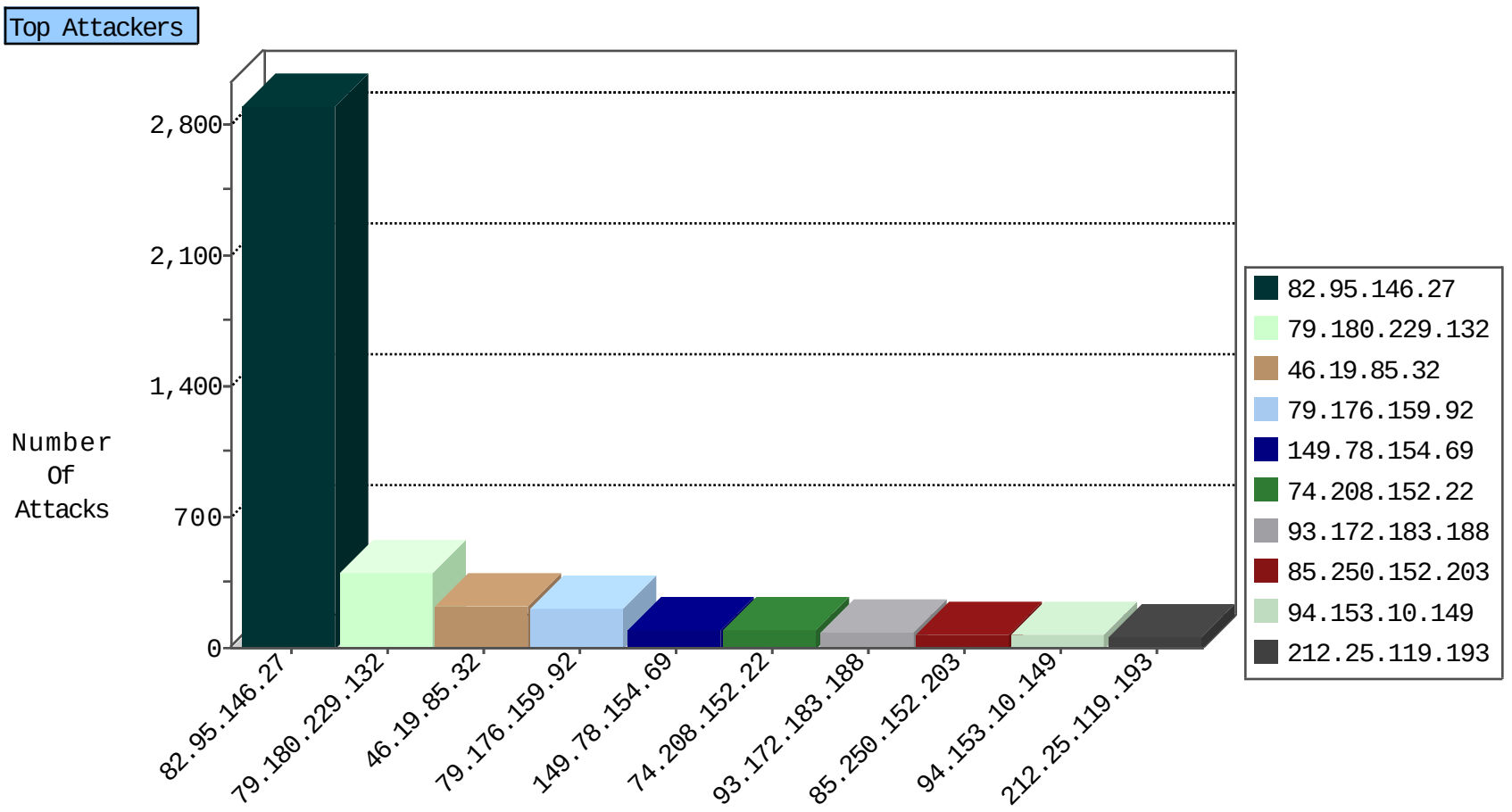
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-31-2015-15:04:08 to 10-31-2015-16:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.92	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6688
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3162
79.176.159.92	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	2843
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	257
2.54.176.132	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	55
46.19.86.103	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	32
85.250.152.203	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
85.64.158.215	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
2.54.19.150	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
79.181.28.247	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
176.12.149.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
2.52.1.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
176.12.146.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.19.85.32	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.19.86.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
46.120.28.83	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
149.78.118.135	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
84.228.176.100	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
37.26.149.229	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
84.228.127.90	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
37.26.146.251	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
77.125.116.192	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.116.185.39	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.120.213.149	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
185.32.179.116	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.246.139.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
5.28.139.186	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
87.69.30.86	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.12.137.105	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
85.250.12.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.109.69.67	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
159.253.145.183	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
93.173.190.74	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
24.85.204.138	Canada	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.10.115	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.155	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.183.132.216	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4
185.32.179.192	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
178.166.249.110	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.12.146.26	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.26.148.135	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
84.111.111.135	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
185.32.179.192	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
24.171.130.104	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
109.67.61.238	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
5.22.129.133	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
84.110.145.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3

10-31-2015-15:04:08 to 10-31-2015-16:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

10-31-2015-15:04:08 to 10-31-2015-16:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

10-31-2015-15:04:08 to 10-31-2015-16:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	207
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
93.172.183.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
85.250.152.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
2.54.4.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
31.154.168.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
149.88.11.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
62.140.137.106	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
82.145.220.19	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
100.100.103.223		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
89.138.83.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
84.229.145.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.86.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
82.81.28.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
168.235.195.72	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.52.1.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
82.95.146.27	Netherlands	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
223.176.159.62	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.26.146.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.73.227		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
79.178.173.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.158.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.82.160		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
5.22.129.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.24.40		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
217.197.39.28	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
84.111.104.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.54.176.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
176.13.7.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.120.28.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.241.239.195	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.54.19.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.16.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.95.146.27	Netherlands	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2842
79.180.229.132	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	405
74.208.152.22	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 74.208.152.22	Block	75
84.108.240.10	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 84.108.240.10	Block	49
94.153.10.149	Ukraine	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 94.153.10.149	Block	45
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	45
82.95.146.27	Netherlands	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	45
212.25.119.193	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	30
80.178.190.35	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	30
176.12.150.221	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	30
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	30
212.25.119.193	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	30
79.183.38.202	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	15
66.249.67.232	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	15
157.55.39.106	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/chinuch/faq/default.asp	None	15
83.220.53.30	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1283-en/dover.aspx	Block	15
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
79.179.21.174	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	15
185.120.126.1		147.237.77.216	dover.idf.il	NULL Character in Method	Block	15
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3208.pdf	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
74.208.152.22	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	15
176.12.143.9	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/1923.pdf	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
83.220.53.30	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1283-en/dover.aspx	Block	15
46.120.49.251	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	15
79.179.141.229	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	15
187.121.3.74	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	15
66.249.79.242	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/sip_storage/files/8/3208.pdf	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/haredim/general.aspx	Block	15
94.153.10.149	Ukraine	147.237.76.42	refuah.idf.il	PHP Attempt	Block	15
5.29.226.160	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	15
79.176.222.59	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	15
176.12.148.2	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
66.249.78.128	Israel	147.237.76.147	chinuch.aka.idf.i	Suspicious Response Code_Custom_Temporary	Block	15
66.249.65.139	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/ajaxpage.aspx	Block	15
207.46.13.70	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	15
68.42.33.110	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	15
94.153.10.149	Ukraine	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	15
37.26.147.159	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	15
79.177.190.209	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pniasubmittedsuccessfully.aspx	None	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	15
93.172.142.250	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
79.181.20.25	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	15
66.249.67.232	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 66.249.67.232 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	15
157.55.39.86	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	15
83.220.53.30	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	15
37.26.148.135	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
79.177.190.209	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	15