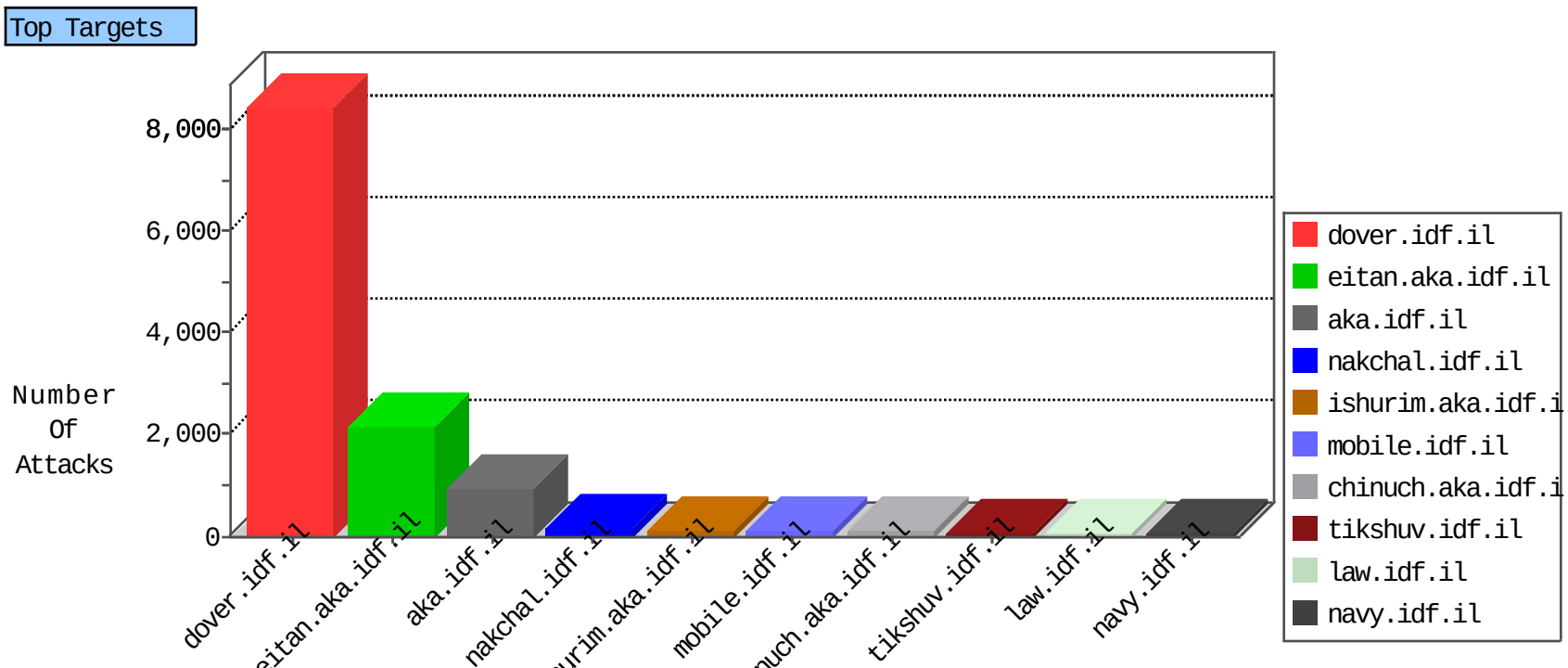
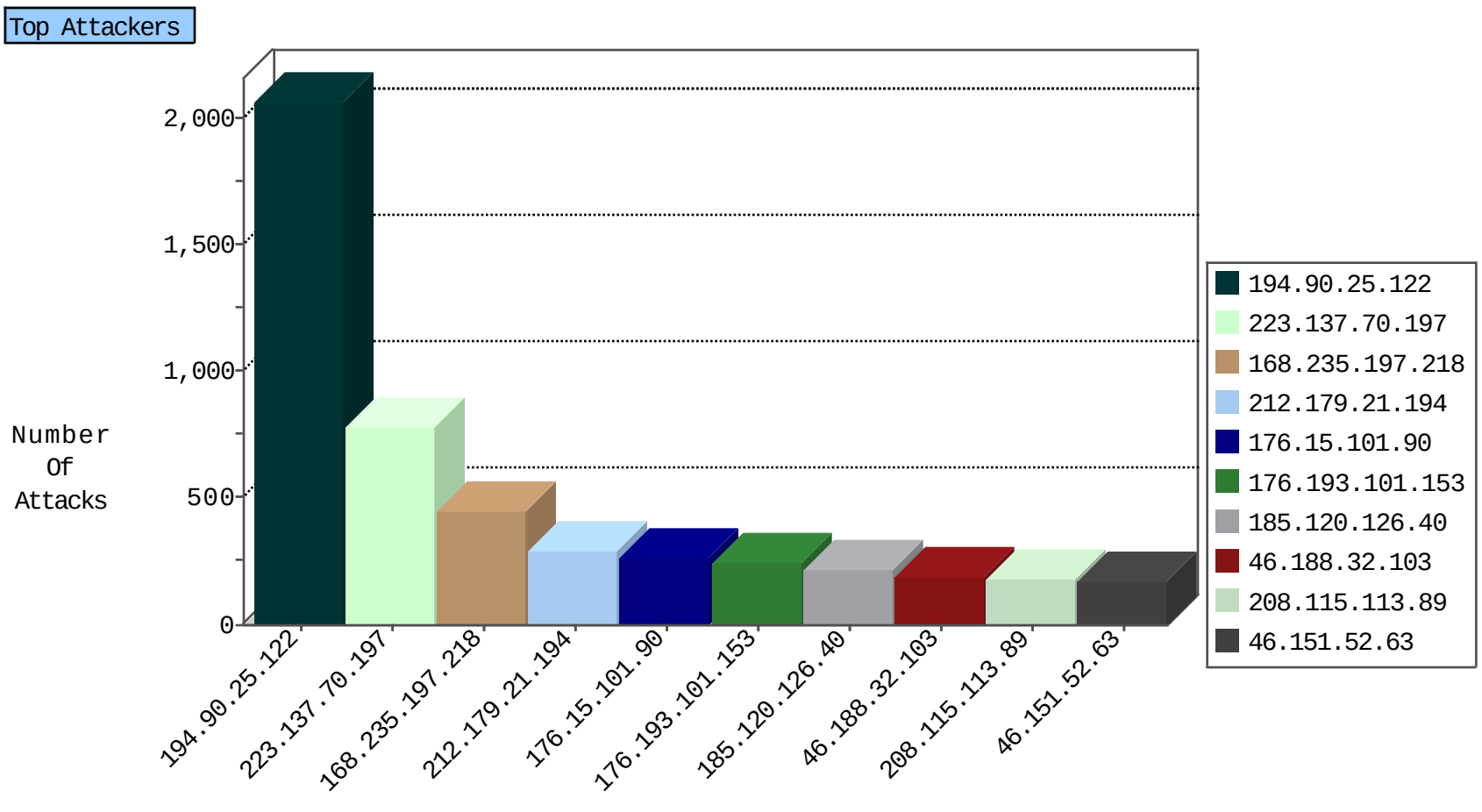
10-22-2015-10:04:00 to 10-22-2015-11:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-22-2015-10:04:00 to 10-22-2015-11:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.235.197.218	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2987
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	203
176.13.15.55	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	42
46.116.132.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
80.74.107.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
5.102.254.168	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
77.125.126.38	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
81.218.124.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
166.172.191.189	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
46.116.119.87	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
84.111.225.210	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.186.37.172	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
31.168.100.81	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
213.151.32.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.66.157.3	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.181.2.126	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.52.139.191	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
82.102.169.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
93.173.29.13	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.137.63	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.193.101.153	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
46.19.85.62	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.29.82	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
79.177.173.36	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
213.8.44.227	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.86.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.13.0.139	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
81.218.124.66	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
176.13.2.84	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
142.54.187.46	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
176.12.141.171	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
223.137.70.197	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
176.12.143.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
54.163.10.122	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.248.172.98	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
213.57.81.82	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
142.54.172.107	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
54.187.251.165	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
185.32.179.121	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
173.208.168.163	United States	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1

10-22-2015-10:04:00 to 10-22-2015-11:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.117.143.250	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6

10-22-2015-10:04:00 to 10-22-2015-11:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
2.229.240.11	147.237.76.196	Italy	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
77.127.173.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.143	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.99.143	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.229.240.11	147.237.76.39	Italy	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
222.33.128.193	147.237.72.14	China	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.179.1.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.174.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
49.73.160.91	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1

10-22-2015-10:04:00 to 10-22-2015-11:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
223.137.70.197	Taiwan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	784
168.235.197.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	440
176.15.101.90	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	260
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	249
176.193.101.153	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	246
185.120.126.40		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	212
46.188.32.103	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	186
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	167
85.181.127.56	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	162
95.25.84.35	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
37.26.146.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
79.177.173.36	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	94
62.90.144.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
212.76.101.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
65.49.68.202	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
73.241.79.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
46.19.86.16	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
80.246.133.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
212.143.248.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
46.19.85.0	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
87.69.88.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
46.19.86.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
166.172.191.189	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
70.199.73.3	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
47.16.244.235	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
212.14.233.93	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
176.13.17.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
176.77.31.187	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
79.183.1.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
2.54.58.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
2.54.2.212	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
94.188.248.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
157.55.39.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
37.73.216.13	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.19.86.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.19.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
52.23.254.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.90.25.122	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 194.90.25.122	Block	2044
85.64.195.249	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.195.249	Block	97
46.151.52.63	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	84
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	81
185.120.126.33		147.237.76.31	nakchal.idf.il	Post Request - Missing Content Type from 185.120.126.33	Block	72
46.151.52.63	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.151.52.63	Block	70
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	56
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	56
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	42
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	42
2.54.173.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	42
176.13.1.138	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	28
46.19.86.17	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	28
195.151.254.213	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
65.55.210.66	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	28
83.223.122.21	United Kingdom	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &y in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	28
185.120.126.33		147.237.76.31	nakchal.idf.il	Post Request - Missing Content Type	Block	15
193.34.57.101	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/haredim/scriptresource.axd	None	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	14
46.151.52.63	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	14
5.29.194.155	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
132.64.182.140	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main/m...91&docid=66007	Block	14
79.183.17.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
212.199.195.219	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 212.199.195.219	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
157.55.39.126	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	14
85.64.151.176	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	14
176.13.11.123	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	14
17.138.54.212	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	14
81.218.183.222	Israel	147.237.72.166	aka.idf.il	Unknown Parameter x in www.aka.idf.il/main/sachar/payslips.aspx	None	14
212.199.195.219	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/164-3447-he	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16552-en/dover.aspx-title=for	Block	14
188.143.232.11	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
157.55.39.237	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19142-en/dover...	Block	14
46.116.223.205	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	14
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1129-he/kkkkkkk=bf6bf9b5kkkkkkk_bf6bf9b5	Block	14
17.138.60.150	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	14
141.212.122.96	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to /x	Block	14
82.166.125.198	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	14
217.194.197.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
188.143.232.15	Russian Federation	147.237.77.176	matpash.idf.il	Distributed Parameter Type Violation on www.cogat.idf.il/901-en/cogat.aspx parameter fromDate	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
176.12.151.128	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
2.54.173.175	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
87.68.38.182	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
203.133.168.29	Korea, Republic of	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
185.120.126.33		147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	14
141.212.122.96	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /x	Block	14
46.19.85.237	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14