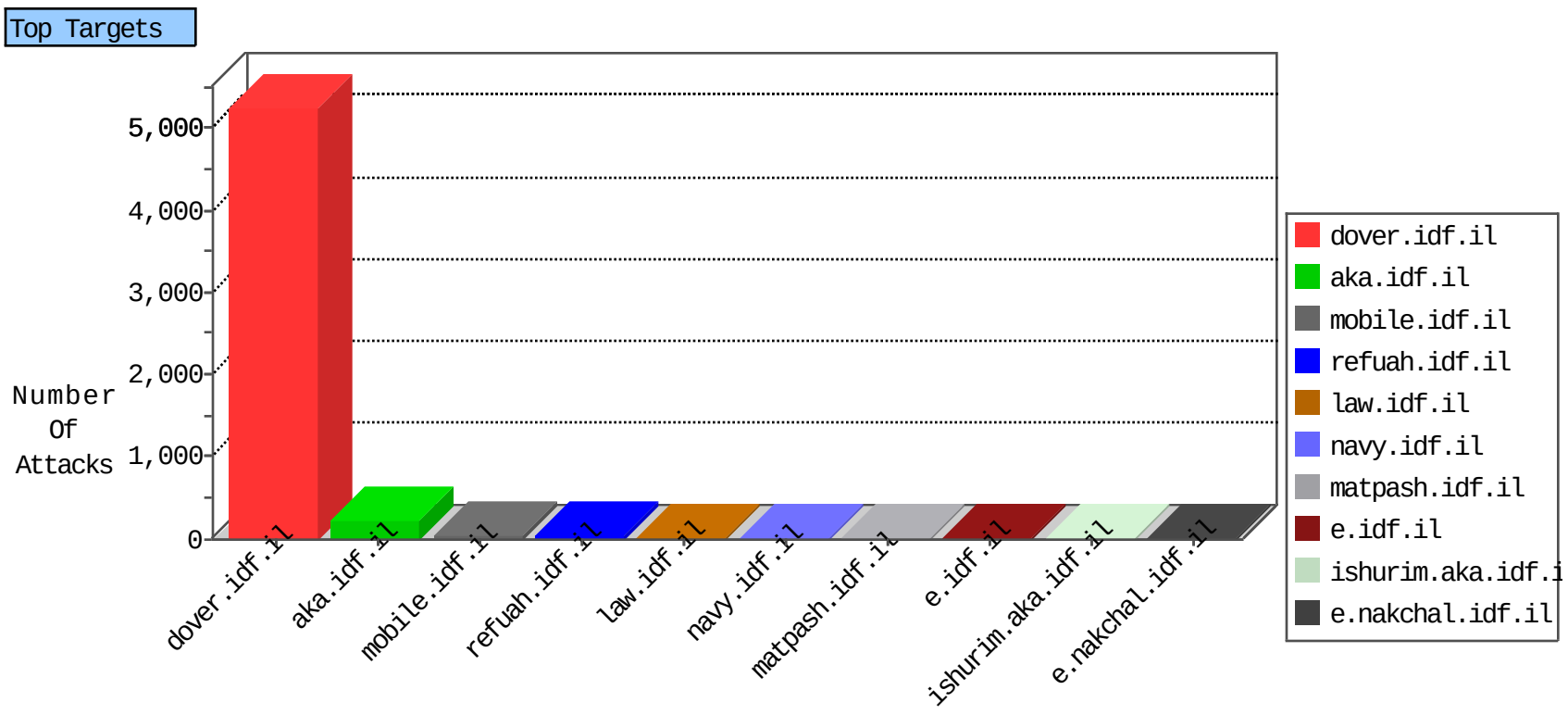
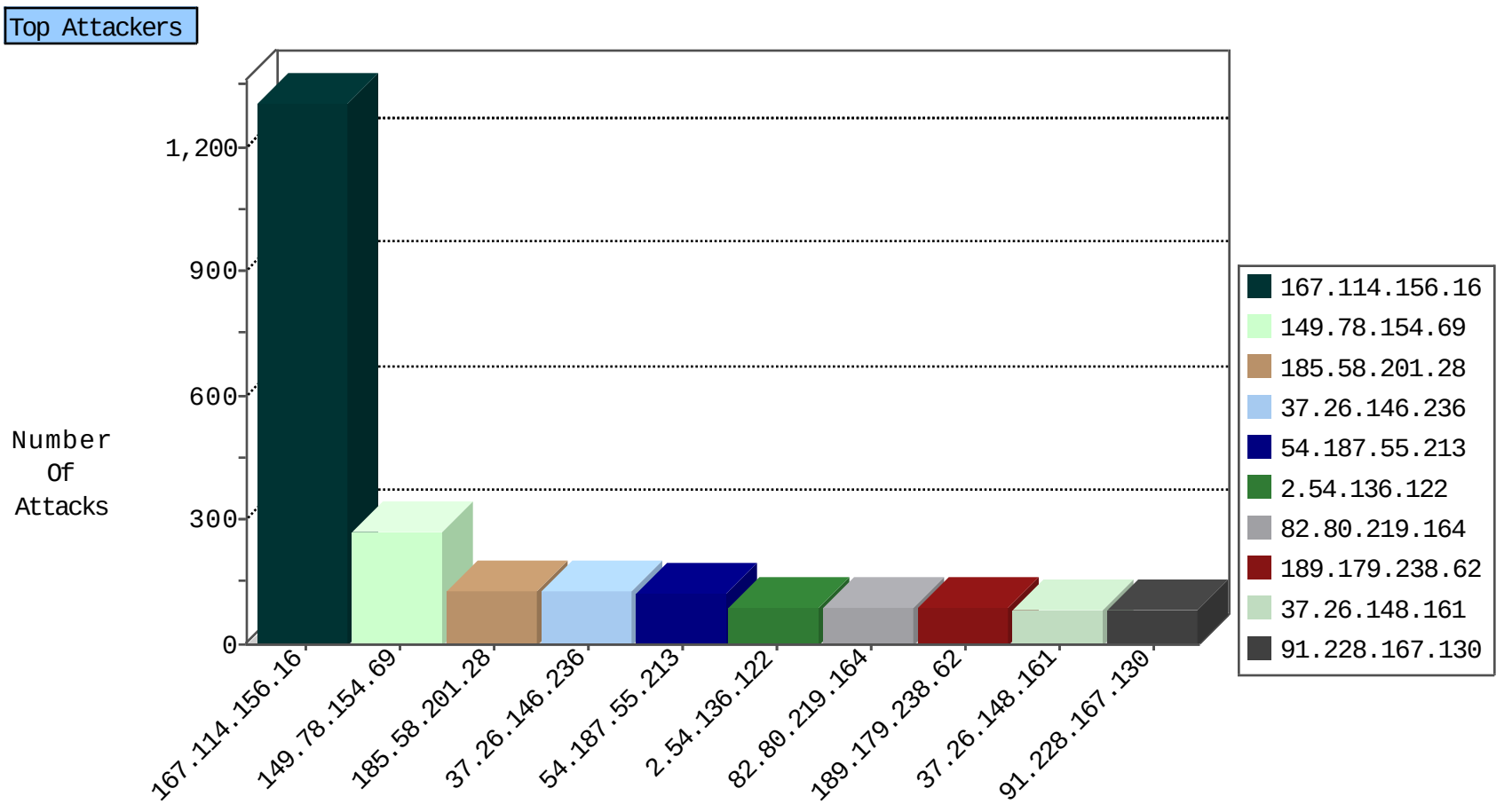
11-02-2015-07:04:08 to 11-02-2015-08:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-02-2015-07:04:08 to 11-02-2015-08:04:08

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	2369
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	148
89.138.94.193	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
176.12.143.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
213.57.46.4	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
82.80.129.76	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.29	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.26.149.162	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.17	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
98.198.104.220	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
203.40.141.41	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
2.52.50.137	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
95.172.79.236	United Kingdom	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
2.54.0.119	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
95.172.79.244	United Kingdom	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
176.13.18.56	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.13.8.139	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.137.211	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
114.200.8.101	Korea, Republic of	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
2.54.0.119	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
183.60.48.25	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
123.193.178.149	Taiwan	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
82.221.105.7	Iceland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
2.54.3.34	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
176.13.14.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
112.175.228.19	Korea, Republic of	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1

11-02-2015-07:04:08 to 11-02-2015-08:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	30
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

11-02-2015-07:04:08 to 11-02-2015-08:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.69.92	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
209.98.225.211	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sA (2)	3
198.20.69.98	147.237.76.198	United States	e.yohalan.idf.i	ET DROP Dshield Block Listed Source	1
46.20.9.25	147.237.76.199	Turkey	e.nakchal.idf.i	ET SCAN NMAP -f -sS	1
193.104.41.54	147.237.76.198	Moldova, Republic of	e.yohalan.idf.i	ET SCAN Potential SSH Scan	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
176.13.20.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.22.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.72.71.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.217.129.145	147.237.8.45	Spain	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.111.158.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.191.100.12	147.237.76.42	China	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
202.79.243.160	147.237.77.216	Japan	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.20.9.25	147.237.76.199	Turkey	e.nakchal.idf.i	ET SCAN NMAP -sS window 1024	1
176.13.23.106	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.55.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
139.204.50.26	147.237.8.46	China	e.chinuch.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
115.132.227.125	147.237.76.38	Malaysia	e.e.meitav.idf.	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
87.69.235.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.102.169.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.20.9.25	147.237.76.199	Turkey	e.nakchal.idf.i	ET SCAN NMAP -sS window 2048	1

11-02-2015-07:04:08 to 11-02-2015-08:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	273
37.26.146.236	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	131
185.58.201.28	Lebanon	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	129
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	122
2.54.136.122	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	89
82.80.219.164	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	88
189.179.238.62	Mexico	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	88
91.228.167.130	Slovakia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	83
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	79
101.190.85.238	Australia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	71
132.72.71.53	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	68
91.228.167.109	Slovakia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	62
70.195.129.3	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	62
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	61
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	58
37.26.148.161	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	55
129.63.96.160	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	54
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
82.102.169.113	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	49
2.54.45.233	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
69.172.160.19	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
149.78.108.210	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
144.76.113.213	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
79.174.225.39	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
2.52.135.4	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
84.111.138.75	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
149.78.148.244	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
46.116.82.17	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
46.116.200.177	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
92.62.170.67	Lebanon	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
176.13.2.36	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
80.179.9.7	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
46.19.85.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.65.193.113	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
95.86.70.171	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
37.26.148.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.181.180.33	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
176.13.11.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
212.199.34.114	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
107.77.70.28	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
176.12.142.248	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
82.80.25.221	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
80.179.9.115	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
192.99.12.99	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
2.52.47.68	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.92	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	6
66.249.69.76	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	4
103.243.64.238	Papua New Guinea	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
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	2
68.180.229.239	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 68.180.229.239	Block	2
66.249.69.84	Israel	147.237.77.74	law.idf.il	Multiple Illegal Parameter Encoding from 66.249.69.84	None	2
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/ge...04	Block	1
66.249.78.66	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
216.218.206.68	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1506-	Block	1
66.249.69.84	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/×œ ×§×©×¨ ×œ×—×œ×§ ×©×ž×¡×'×™×¨ ×¢×œ ×–×"	Block	1
46.19.85.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.147.210	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20140-he/idfgdover.aspx	Block	1
216.223.27.55	United States	147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/../images/shared/home.png	Block	1
109.66.110.215	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1232-he/atal.aspx	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/news/kamlar/mishpaha.jpg+	Block	1
176.13.4.41	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.182.98.43	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aka	Block	1
66.249.69.84	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
109.66.110.215	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatesMonth in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
184.105.139.68	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
80.178.157.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.84	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
2.54.180.159	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	1
176.12.141.106	Israel	147.237.76.42	refuah.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 176.12.141.106	Block	1
66.249.78.59	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
216.218.206.67	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
84.108.51.152	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
37.26.148.140	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
176.12.147.210	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 176.12.147.210 (Unknown SSL Session)	None	1