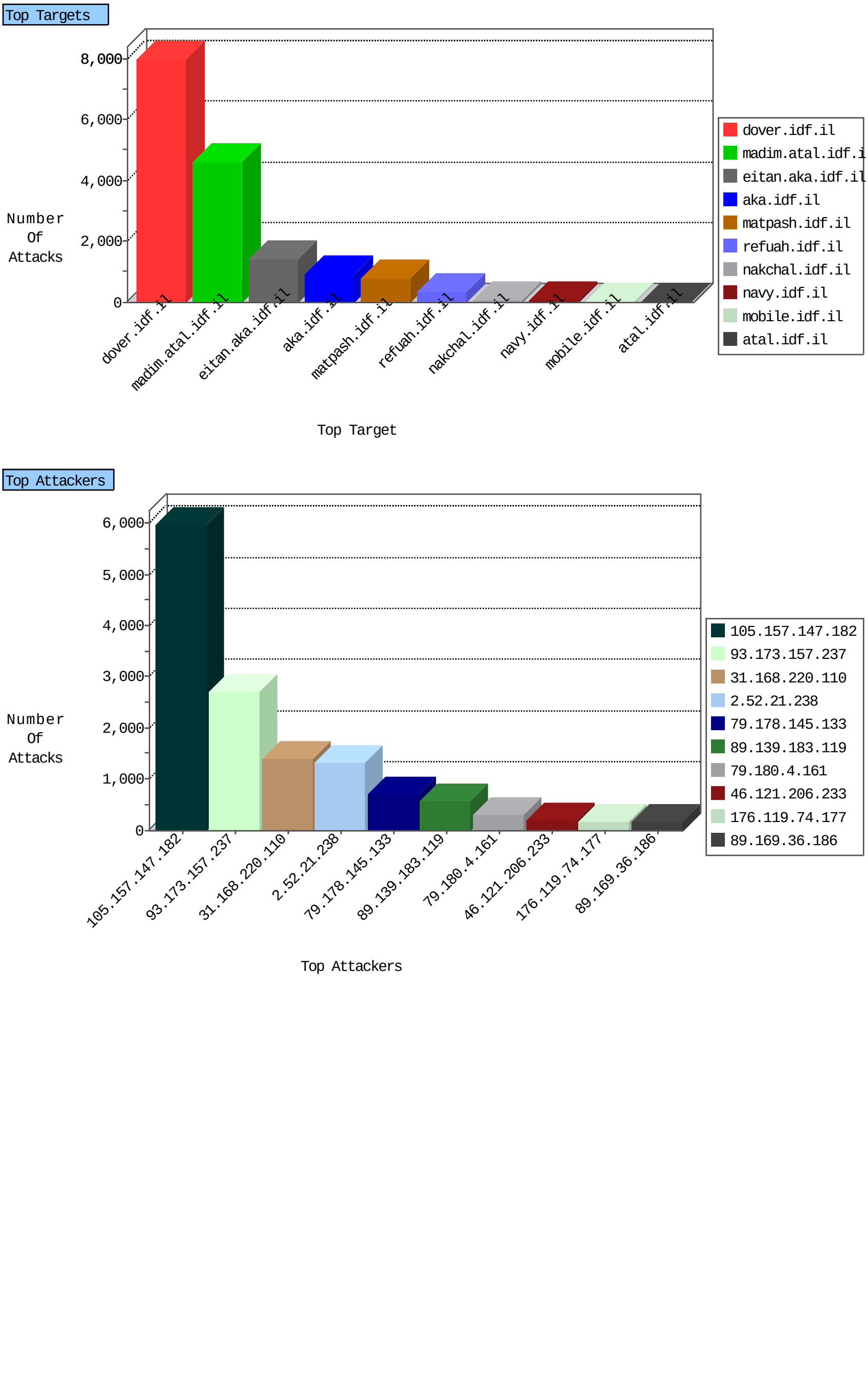
10-24-2015-16:04:04 to 10-24-2015-17:04:04

IDF Under Attack Daily Report



10-24-2015-16:04:04 to 10-24-2015-17:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
109.64.209.241	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
77.125.126.38	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.65.31.35	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
69.248.86.176	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
82.166.86.131	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.139.125	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
87.69.189.146	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.44.1	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
45.32.68.116		147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
142.54.172.99	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1
72.93.4.101	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-24-2015-16:04:04 to 10-24-2015-17:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.205.27	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

10-24-2015-16:04:04 to 10-24-2015-17:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
66.249.67.235	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
198.20.69.74	147.237.76.202	United States	e.halag.idf.il	ET DROP Dshield Block Listed Source	1
188.68.224.151	147.237.8.14	Poland	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
180.149.139.247	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
115.78.119.45	147.237.0.34	Vietnam	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
199.255.138.49	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
199.255.138.49	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
199.255.138.49	147.237.76.31	United States	nakchal.idf.il	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
199.255.138.49	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
199.255.138.49	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
188.68.224.151	147.237.8.14	Poland	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
159.122.232.87	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.48.194	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
199.255.138.49	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.138	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
199.255.138.49	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
199.255.138.49	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
199.255.138.49	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

10-24-2015-16:04:04 to 10-24-2015-17:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
105.157.147.182	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3443
31.168.220.110	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	819
105.157.147.182	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	648
79.180.4.161	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	289
105.157.147.182	Morocco	147.237.77.216	dover.idf.il	drop		drop	130
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	122
46.116.210.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
37.26.148.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
69.248.86.176	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
93.169.156.69	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
5.28.156.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
86.86.180.94	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
100.100.40.149		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
79.178.162.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
109.186.45.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
192.117.8.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
37.142.226.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	28
37.142.191.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	26
46.19.86.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.121.206.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.97.185		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
79.182.1.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
37.142.132.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
126.152.46.85	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
100.100.40.149		147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	20
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
109.67.123.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.117.75.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.102.8.178	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
100.100.100.179		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
37.142.196.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
66.249.67.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
92.22.209.232	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
107.170.61.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.179.129.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.99.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.157.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2711
105.157.147.182	Morocco	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.157.147.182	Block	1558
2.52.21.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1315
79.178.145.133	Israel	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	714
89.139.183.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	574
31.168.220.110	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 31.168.220.110	Block	574
46.121.206.233	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	168
105.157.147.182	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.157.147.182	Block	112
176.119.74.177	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	84
89.169.36.186	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	84
89.169.36.186	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.169.36.186	Block	70
176.119.74.177	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.119.74.177	Block	70
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
79.181.25.141	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.181.25.141 (Unsupported Legacy SSL Version)	None	42
79.181.205.27	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.181.205.27	Block	28
79.181.205.27	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	28
105.157.147.182	Morocco	147.237.77.216	dover.idf.il	Post Request - Missing Content Type	Block	15
105.157.147.182	Morocco	147.237.77.216	dover.idf.il	Post Request - Missing Content Type	Block	15
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	14
176.119.74.177	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	14
89.139.173.132	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	14
207.46.13.7	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
79.180.4.161	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	14
176.13.9.37	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	14
93.172.57.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	14
188.143.232.14	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	14
109.160.236.6	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	14
208.115.111.73	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
176.13.9.37	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.9.37	None	14
66.249.65.181	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	14
84.109.49.174	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14
188.143.232.14	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	14
109.186.60.38	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	14
216.218.206.66	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	14
79.181.25.141	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unsupported Legacy SSL Version	None	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	14
85.64.72.212	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
79.176.105.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
188.165.15.205	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-5486-he/patzar.aspx	Block	14
169.45.161.177	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	14
79.181.107.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	14
85.250.234.4	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/scripts/css3pie.htc	Block	14
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/16946.jpg	Block	14
176.13.4.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	14
46.19.86.34	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.19.86.34	Block	14
89.169.36.186	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	14