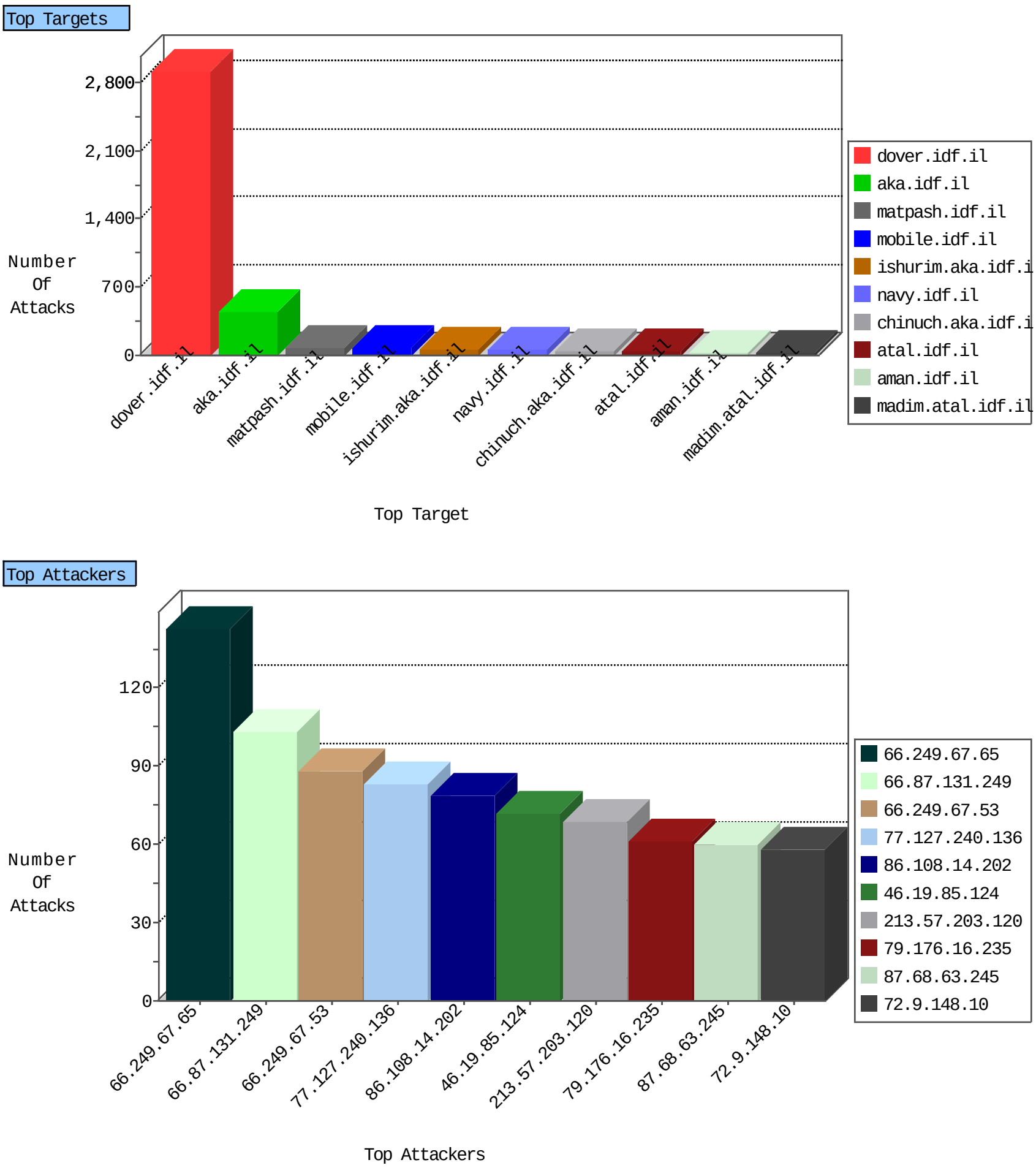
10-24-2015-22:04:03 to 10-24-2015-23:04:03

IDF Under Attack
Daily Report



10-24-2015-22:04:03 to 10-24-2015-23:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	666
85.65.62.86	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
2.54.139.84	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	27
185.27.105.186	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
213.57.215.159	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
46.19.86.30	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	8
82.166.22.87	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.117.177.154	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
77.127.62.180	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.139.84	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
79.182.110.77	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
185.24.207.13	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
210.186.181.234	Malaysia	147.237.77.234	halag.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
46.19.86.99	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.135.131	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
222.186.56.42	China	147.237.76.38	e.e.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
109.67.19.23	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
185.32.179.209	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
176.106.44.191	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.6.135.131	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

10-24-2015-22:04:03 to 10-24-2015-23:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-24-2015-22:04:03 to 10-24-2015-23:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.124	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	54
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
66.249.67.79	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	3
5.22.131.89	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2
5.22.131.89	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
112.216.109.98	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.8	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.25.83	147.237.77.179	France	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
188.68.224.151	147.237.76.30	Poland	himush.idf.il	ET SCAN NMAP -sS window 1024	1
157.55.80.72	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
5.8.66.90	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
112.216.109.98	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
112.216.109.98	147.237.0.19	Korea, Republic of	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
112.216.109.98	147.237.0.16	Korea, Republic of	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
188.68.224.151	147.237.76.30	Poland	himush.idf.il	ET SCAN NMAP -sS window 3072	1
171.249.103.126	147.237.8.50	Vietnam	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.216.109.98	147.237.0.200	Korea, Republic of	m4u.idf.il	ET SCAN Potential SSH Scan	1
112.216.109.98	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Potential SSH Scan	1

10-24-2015-22:04:03 to 10-24-2015-23:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.87.131.249	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
77.127.240.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
86.108.14.202	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
213.57.203.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
79.176.16.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
87.68.63.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
104.34.105.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
87.68.39.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
71.206.29.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
89.139.2.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
187.180.14.37	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
109.186.144.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
141.0.14.145	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
199.58.81.144	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
46.19.86.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
2.52.1.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
200.192.79.12	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
68.180.230.29	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	31
109.186.146.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
77.125.116.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
46.19.86.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
79.180.33.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
37.26.146.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
89.139.175.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
84.228.61.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
105.156.35.126	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
213.57.138.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
85.130.216.252	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.124	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
79.176.193.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
31.210.187.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
2.54.139.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
31.168.83.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.64.8.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.54.153.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.106.226.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
5.28.143.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.67.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.66.191.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14

10-24-2015-22:04:03 to 10-24-2015-23:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	98
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	66
199.16.156.126	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.16.156.126	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
5.29.219.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
66.249.93.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyu	Block	14
40.77.167.44	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	14
199.16.156.124	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/0/size220x0/16900.jpg	Block	14
109.67.52.138	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	14
79.178.119.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
218.189.26.20	Hong Kong	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1393-en/dover.aspx parameter ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker	Block	14
52.91.173.216	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/scrollpanebottom.gif)	Block	14
183.79.219.111	Japan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
87.68.21.145	Israel	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	14
40.77.167.45	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	14
149.202.62.90	Germany	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1393-en/dover.aspx	Block	14
79.181.27.141	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/g.aspx	Block	14
183.160.241.48	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/account/signup/	Block	14
5.102.207.200	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.102.207.200	Block	14
109.65.9.30	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9237-he/refuah.aspx	Block	14
46.19.85.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	14
207.46.13.144	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
176.10.104.234	Switzerland	147.237.77.176	matpash.idf.il	Distributed Parameter Type Violation on www.cogat.idf.il/901-en/cogat.aspx parameter fromDate	Block	14
5.29.135.205	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
80.246.133.132	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	14
5.102.207.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/6_s3_	Block	14
188.143.232.62	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	14
109.65.104.195	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	14
46.116.69.76	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	14
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18764-en/	Block	14
176.10.104.234	Switzerland	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	14
5.29.135.205	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	14
82.166.22.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
40.77.167.43	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	14
197.249.49.231	Mozambique	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1393-en/dover.aspx parameter ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker	Block	14
109.66.170.199	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	14
212.199.143.202	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	14
46.121.133.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
176.13.8.187	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	14
5.29.219.141	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	14
84.228.130.120	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
79.177.201.237	Israel	147.237.0.16	my-kosher-kravi.idf.il	Parameter Type Violation Master$ContentPlaceHolder1$distance in my-kosher-kravi.idf.il/ajax/reserveschedule/trainingformiframe.aspx	Block	13

10-24-2015-22:04:03 to 10-24-2015-23:04:03