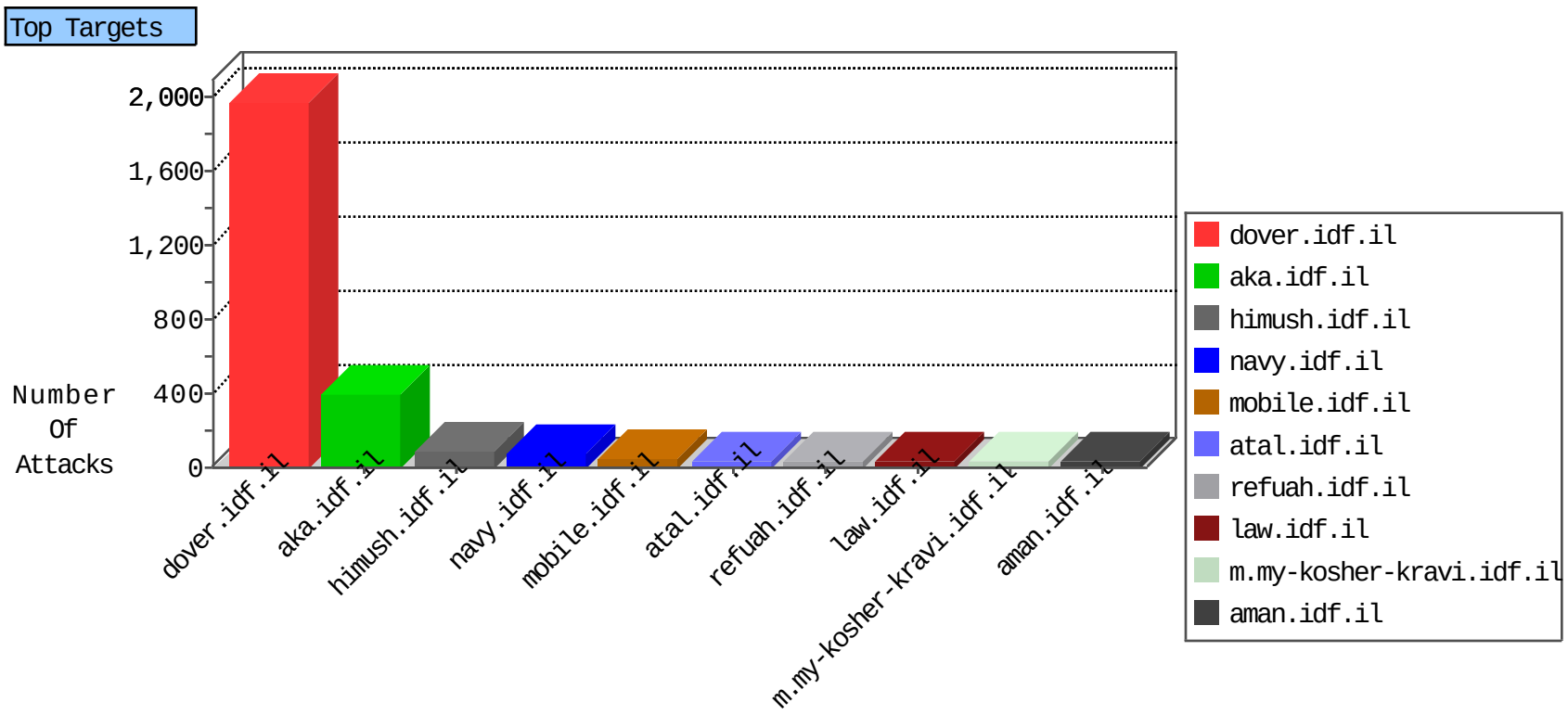
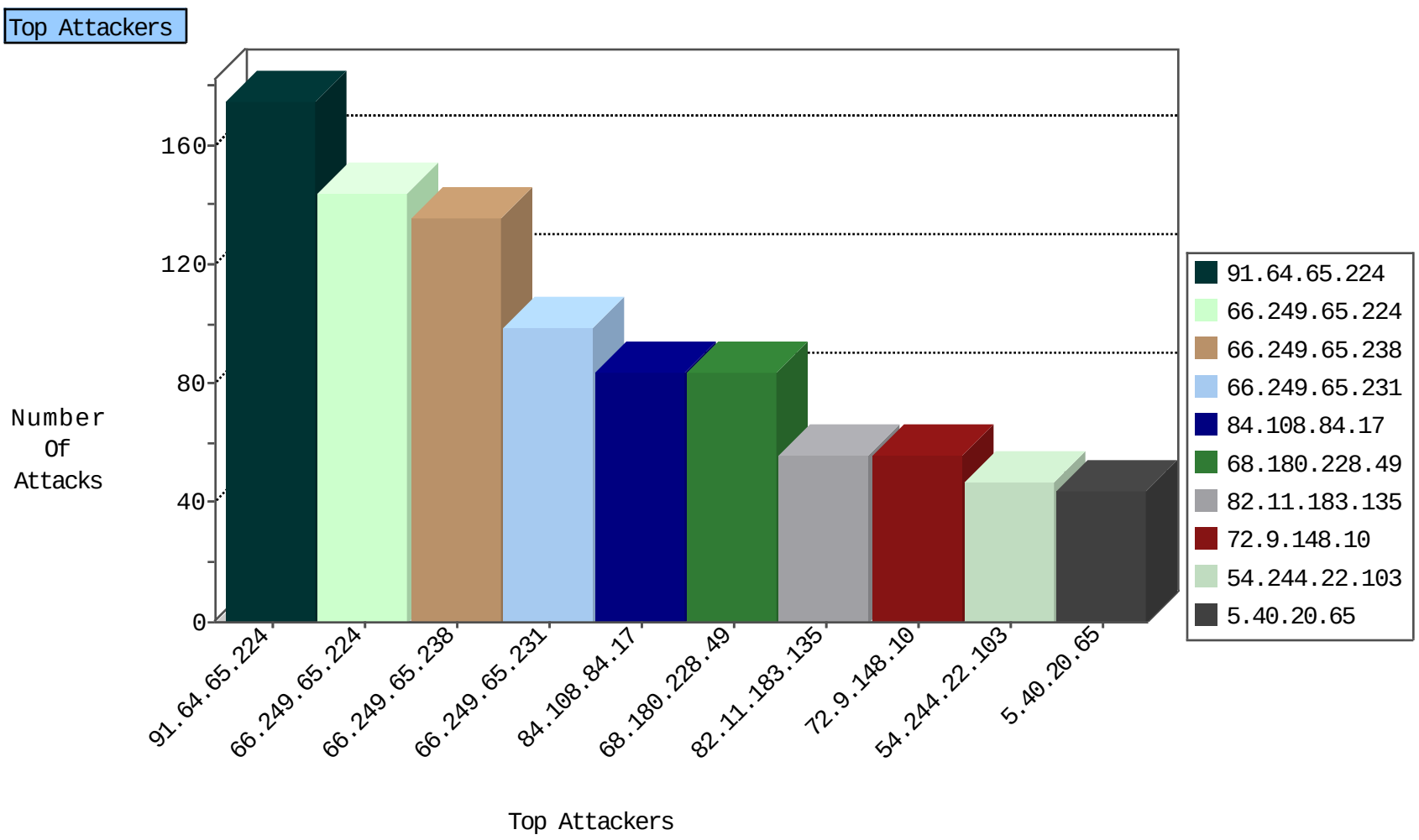
10-23-2015-19:04:01 to 10-23-2015-20:04:01

IDF Under Attack Daily Report





10-23-2015-19:04:01 to 10-23-2015-20:04:01

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	75
176.13.14.7	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	52
87.68.69.137	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	34
85.64.7.50	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
100.40.173.233	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
2.54.179.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
82.11.183.135	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
109.66.182.105	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
2.54.128.237	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
46.116.44.253	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
82.11.183.135	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
109.226.17.214	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
85.250.12.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
148.73.111.9	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
83.171.151.156	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
83.171.151.156	Germany	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
77.127.183.168	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
5.29.91.232	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
148.73.111.9	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
85.64.7.50	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
84.228.80.86	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
84.108.187.161	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
190.104.173.38	Paraguay	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
5.29.141.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
95.35.199.174	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
2.54.128.237	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
95.35.199.174	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
2.54.128.237	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.177.146.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
91.64.65.224	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
185.120.126.39		147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
31.186.178.245	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
46.19.85.25	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
176.13.5.203	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.179.129	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
187.127.59.123	Brazil	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
82.205.114.245	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.19.85.25	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
85.64.108.253	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.116.44.253	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
95.35.199.174	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.116.44.253	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
84.228.80.86	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
173.71.35.54	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
79.181.169.251	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
142.54.172.102	United States	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
85.64.7.50	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
82.205.114.245	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
185.120.126.39		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
148.73.111.9	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
77.127.183.168	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
109.67.142.172	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-23-2015-19:04:01 to 10-23-2015-20:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-23-2015-19:04:01 to 10-23-2015-20:04:01

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	9
176.58.116.93	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
139.162.158.25	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
45.79.157.210	147.237.77.233		atal.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
5.143.82.242	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
210.61.150.154	147.237.72.217	Taiwan	e.idf.il	ET SCAN NMAP -sS window 3072	1
190.124.35.115	147.237.77.235	Nicaragua	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
176.58.112.41	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential SSH Scan	1
117.135.163.104	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
45.79.157.210	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
190.124.35.115	147.237.77.235	Nicaragua	sviva.idf.il	ET SCAN NMAP -sS window 3072	1

10-23-2015-19:04:01 to 10-23-2015-20:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
5.40.20.65	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
76.209.21.60	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
82.11.183.135	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
173.71.35.54	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
187.127.59.123	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
63.116.61.253	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
204.111.204.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
79.183.191.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.116.44.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
79.183.54.82	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
176.13.14.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
12.199.96.253	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.179.36.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
80.179.93.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
12.40.220.253	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
40.77.167.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
130.193.244.216	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
190.104.173.38	Paraguay	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
100.100.63.69		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
194.151.190.5	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
93.173.178.150	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
109.66.182.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.142.200.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
148.73.111.9	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
149.130.222.197	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
105.106.140.174	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.65.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.64.99.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.177.132.187	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
100.100.105.249		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
96.44.189.100	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.186.60.38	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

10-23-2015-19:04:01 to 10-23-2015-20:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.64.65.224	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	168
84.108.84.17	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	84
68.180.228.49	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	84
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	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
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	42
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	28
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	28
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	28
79.183.56.71	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	14
66.249.67.204	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1664	Block	14
146.185.234.48	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/links/links.aspx/templates/sendtofriend/sendtofriend.aspx	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
85.250.5.85	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
79.176.49.186	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily_	Block	14
194.151.190.5	Netherlands	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.151.190.5	Block	14
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
109.66.58.84	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	14
79.183.227.92	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
66.249.67.219	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	14
46.19.85.251	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
79.178.9.161	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	14
66.249.64.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	14
109.66.200.116	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
80.179.225.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/default.aspx tafkidim	Block	14
66.249.73.181	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on 147.237.77.74/robots.txt	Block	14
151.80.31.140	Italy	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	14
46.19.86.56	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 46.19.86.56	Block	14
95.35.192.101	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding {@CWX*kn7BIz]A70E0mt64vCiyD:BWn[S9-A2q	None	14
79.179.117.231	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	14
109.186.60.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
180.76.15.134	China	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	14
46.121.68.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
95.35.192.101	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 95.35.192.101	None	14
79.183.14.85	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	14
137.116.71.170	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
66.249.65.51	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	14
84.228.55.70	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	14
188.165.15.121	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list3.htm	Block	14
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
66.249.64.53	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on 147.237.77.170/robots.txt	Block	14
109.64.103.155	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
194.151.190.5	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/uk	Block	13
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12

10-23-2015-19:04:01 to 10-23-2015-20:04:01