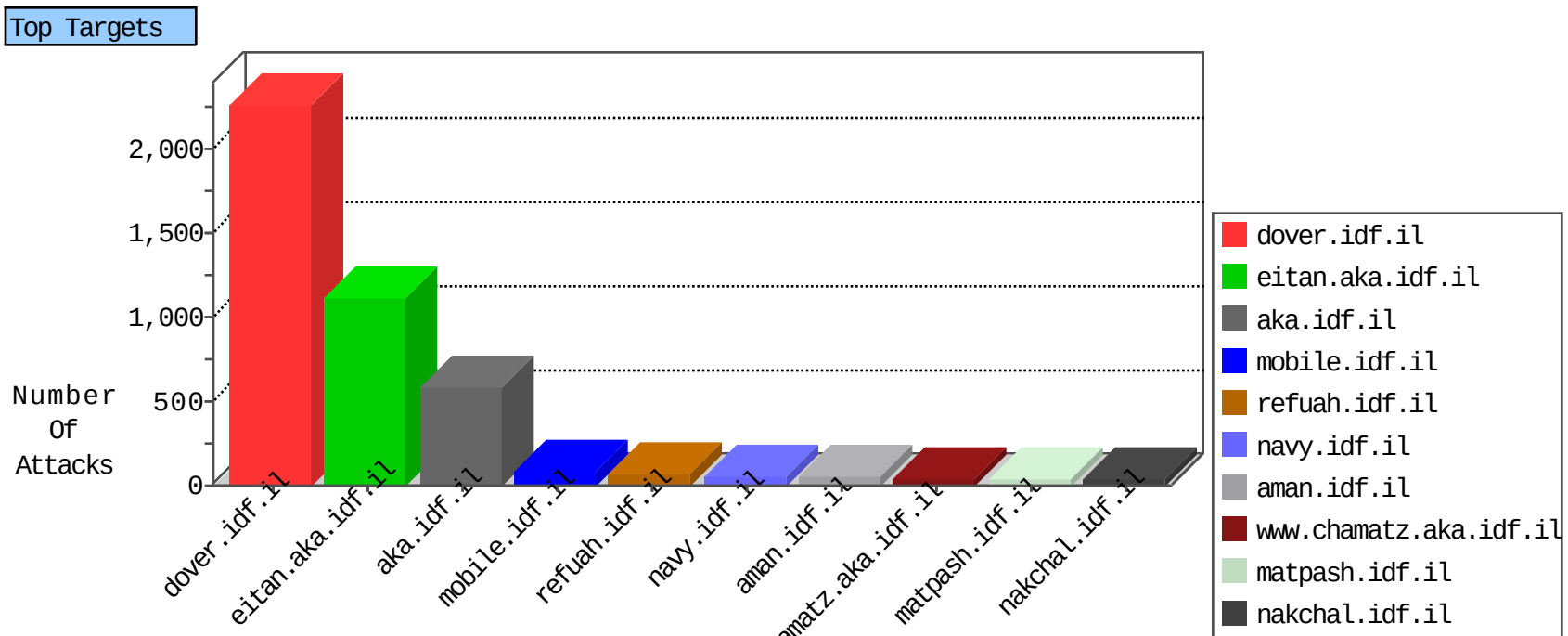
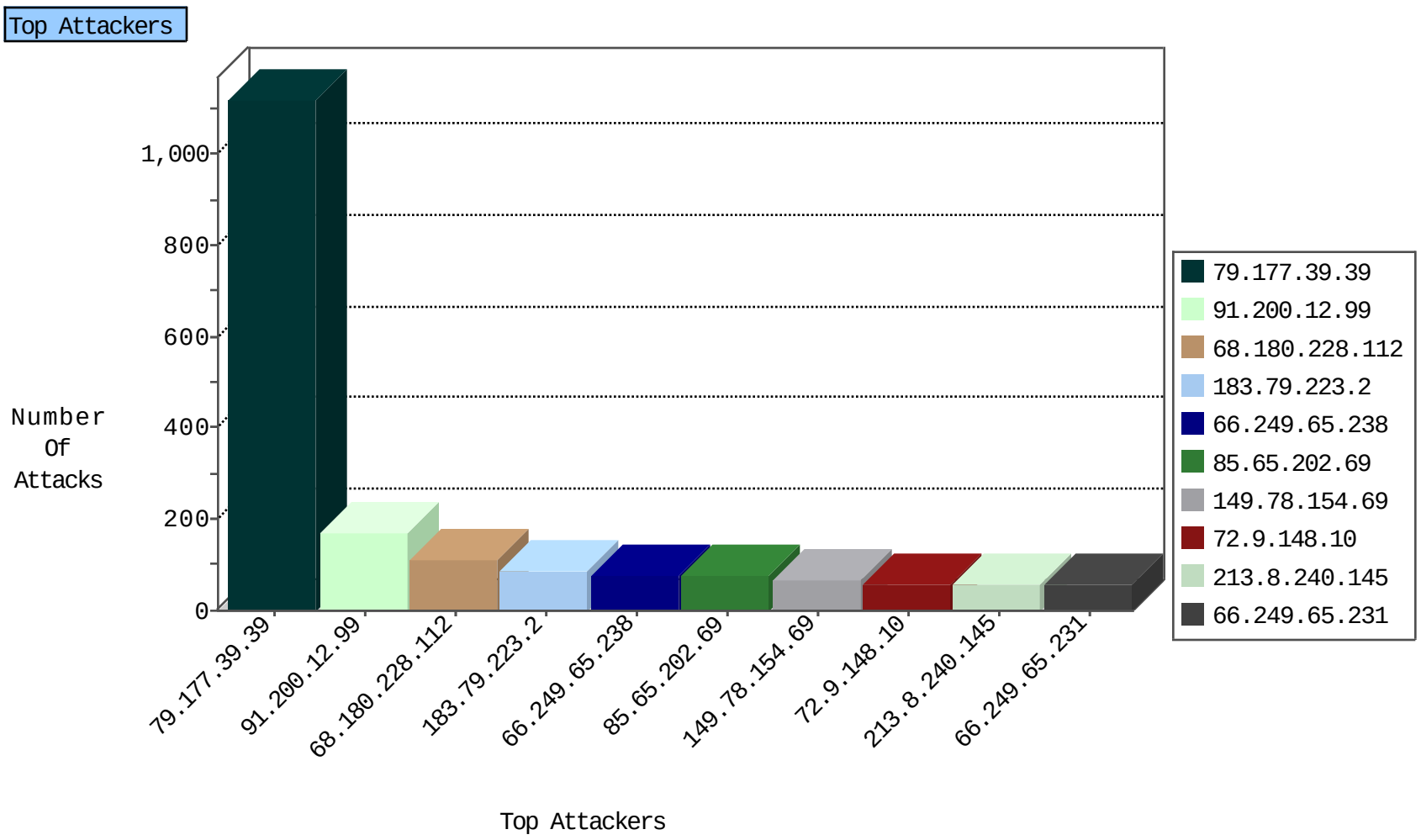
10-24-2015-12:04:01 to 10-24-2015-13:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-24-2015-12:04:01 to 10-24-2015-13:04:01

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.i	SYN Flood full table	drop	80
31.168.116.98	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	48
5.102.212.7	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	13
182.69.132.88	India	147.237.77.216	dover.idf.i	SYN Flood full table	drop	12
31.154.163.69	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
79.182.9.37	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	7
87.69.124.111	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	7
79.179.121.113	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
31.154.91.137	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
5.29.104.173	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	5
84.109.192.159	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
79.178.28.197	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
109.186.180.69	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
2.54.157.166	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	4
109.186.30.130	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
2.52.31.53	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
37.142.140.53	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	4
46.43.117.173	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	SYN Flood full table	drop	3
84.228.177.186	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	3
85.250.90.181	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	3
84.228.106.251	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	2
212.14.228.206	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	SYN Flood full table	drop	2
84.109.32.36	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	2
176.12.146.197	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	2
37.26.146.204	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	2
84.228.56.153	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	2
83.112.222.139	France	147.237.77.216	dover.idf.i	SYN Flood full table	drop	1
37.142.140.53	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	1
2.54.7.103	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	1
94.139.128.198	Moldova, Republic of	147.237.77.216	dover.idf.i	SYN Flood full table	drop	1
213.57.222.143	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	1
76.121.196.159	United States	147.237.77.216	dover.idf.i	SYN Flood full table	drop	1
176.13.22.179	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	1
82.80.25.221	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1
5.29.104.173	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	1
109.186.30.130	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	1
2.52.31.53	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	1

10-24-2015-12:04:01 to 10-24-2015-13:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4

10-24-2015-12:04:01 to 10-24-2015-13:04:01

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	6
87.69.241.92	147.237.72.156	Israel	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
182.48.105.216	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
182.48.105.216	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.49.7	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.64.67.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

10-24-2015-12:04:01 to 10-24-2015-13:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.177.39.39	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	462
85.65.202.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
213.8.240.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
37.142.224.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	49
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
176.13.19.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
37.26.148.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
82.166.84.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
197.160.89.204	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
82.173.178.161	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
85.250.12.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
31.168.116.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
94.139.128.198	Moldova, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
37.142.231.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	26
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
79.182.9.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
37.142.235.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	23
100.100.105.26		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
31.154.163.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
185.32.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
76.121.196.159	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
80.246.133.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
68.148.30.0	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
119.226.71.50	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.239.143.65	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
84.228.207.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
5.102.212.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
62.150.181.16	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
82.102.231.21	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.179.121.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
100.100.13.38		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
109.66.128.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.174.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.69.172	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
85.250.90.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
176.12.144.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.39.39	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	658
91.200.12.99	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	84
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	84
183.79.223.2	Japan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	70
91.200.12.99	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.200.12.99	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
176.13.9.49	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	42
188.143.232.41	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 188.143.232.41	Block	28
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.231	Block	28
156.171.65.213		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en	Block	28
213.57.155.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
37.239.101.234	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	28
66.249.65.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	14
149.78.20.245	Israel	147.237.72.166	aka.idf.il	Unknown Parameter utm_source in www.aka.idf.il/main/home/default.aspx	None	14
84.228.24.157	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/mivtza	Block	14
66.249.65.248	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/894-he	Block	14
178.248.250.125	Czech Republic	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	14
46.117.154.13	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	14
74.82.47.2	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	14
188.143.232.41	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1319-he/	Block	14
149.88.54.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
5.29.119.21	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14
85.65.239.164	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	14
66.249.79.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
178.254.50.101	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	14
91.200.12.99	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	14
188.165.15.121	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list1.htm	Block	14
31.13.102.99	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	14
87.69.86.182	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	14
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/style/shared/datepicker.css	Block	14
109.66.8.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/	Block	14
79.181.97.40	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	14
89.71.127.32	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	14
69.58.178.58	United States	147.237.76.31	nakchal.idf.il	Distributed Suspicious Response Code	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	14
184.105.139.67	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	14
149.78.20.245	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;utm_campaign in www.aka.idf.il/	None	14
82.102.231.21	Palestinian Territory, Occupied	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/657-en/patzar.aspx	Block	14
216.16.138.182	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	14
176.13.21.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
46.19.85.22	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	14
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	11