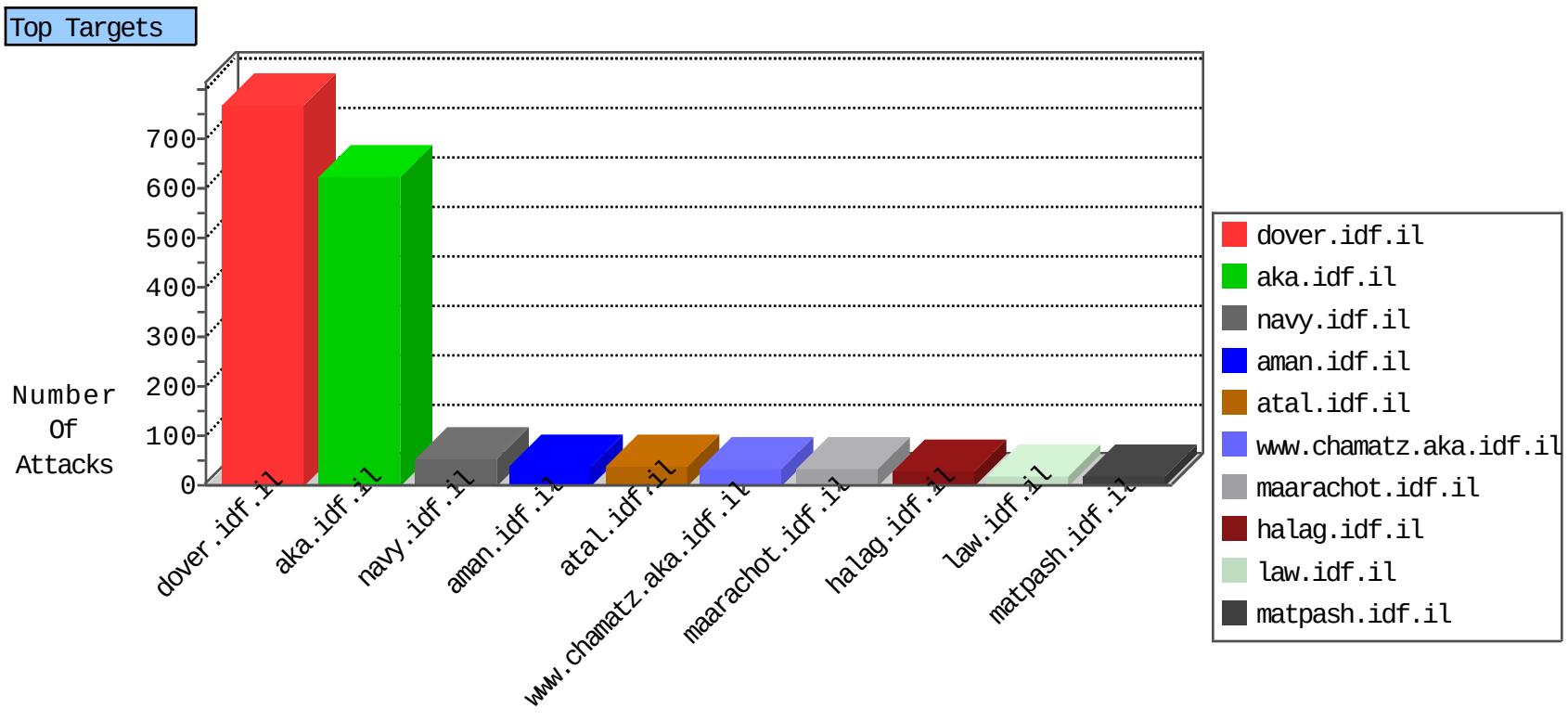
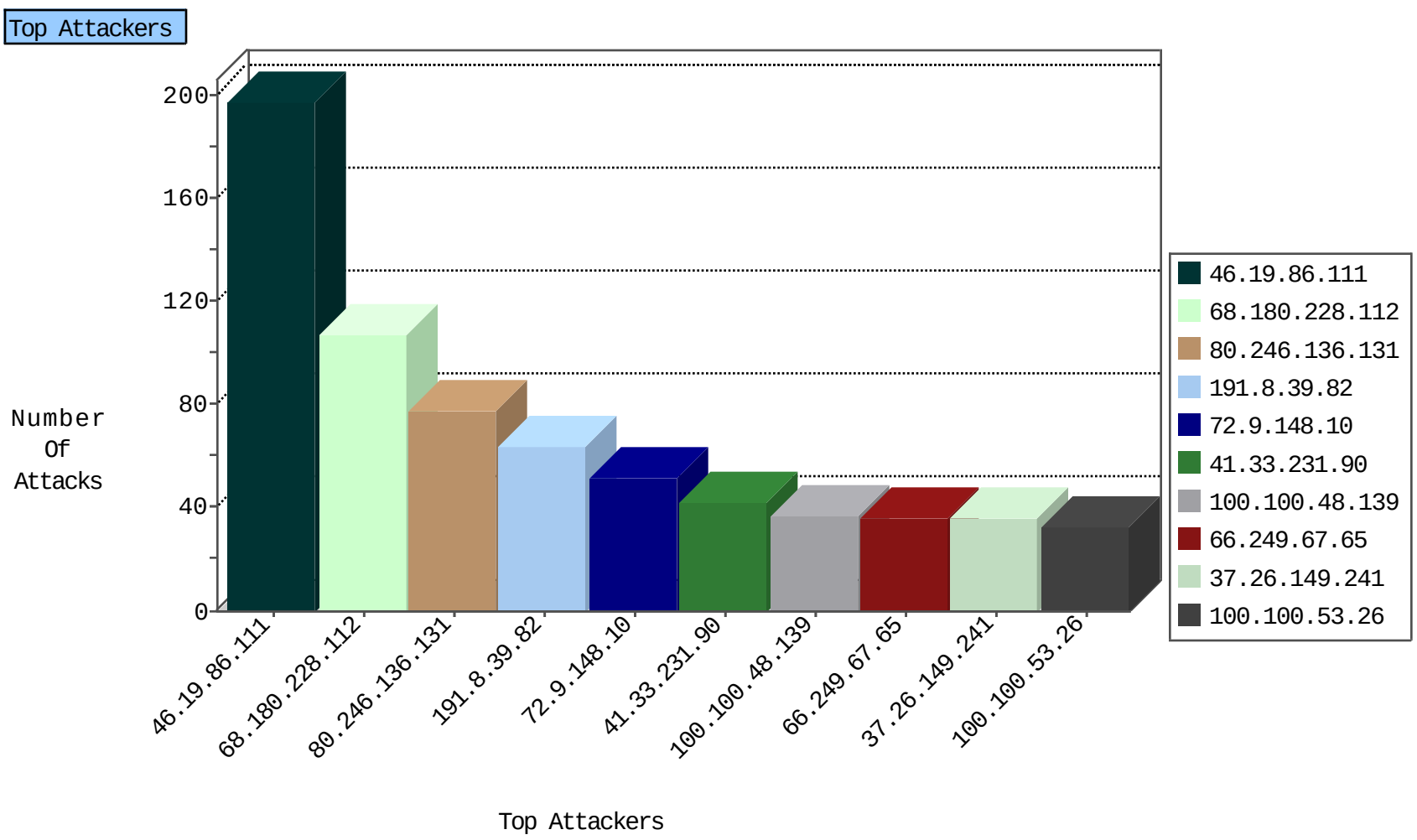
10-21-2015-00:04:08 to 10-21-2015-01:04:08

IDF Under Attack Daily Report





10-21-2015-00:04:08 to 10-21-2015-01:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.31.183	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
71.30.0.65	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
84.108.129.165	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
62.128.35.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
204.28.110.118	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
204.112.35.61	Canada	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
166.172.57.17	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
93.174.93.146	Netherlands	147.237.0.19	madim.atal.idf.il	Invalid TCP Flags	drop	1
93.174.93.146	Netherlands	147.237.76.177	ncore.idf.il	Invalid TCP Flags	drop	1
204.28.110.118	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
93.174.93.146	Netherlands	147.237.76.196	e.sviva.idf.il	Invalid TCP Flags	drop	1

10-21-2015-00:04:08 to 10-21-2015-01:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-21-2015-00:04:08 to 10-21-2015-01:04:08

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
192.240.155.234	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
159.226.230.13	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
177.87.168.30	147.237.72.14	Brazil	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
119.10.8.133	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
159.226.230.13	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
114.233.196.147	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
159.226.230.13	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
159.226.230.13	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
159.226.230.13	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
159.226.230.13	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
218.54.149.67	147.237.72.166	Korea, Republic of	aka.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
159.226.230.13	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
159.226.230.13	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
192.240.155.234	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
119.10.8.133	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
177.87.168.30	147.237.72.14	Brazil	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
119.10.8.133	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
159.226.230.13	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
79.181.67.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
159.226.230.13	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
5.148.157.229	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN NMAP -sS window 1024	1
159.226.230.13	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
159.226.230.13	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
159.226.230.13	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
218.54.149.67	147.237.72.156	Korea, Republic of	aman.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
159.226.230.13	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1

10-21-2015-00:04:08 to 10-21-2015-01:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	198
191.8.39.82	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
100.100.48.139		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	37
100.100.53.26		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	33
37.26.149.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
107.167.113.127	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
46.19.86.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
38.112.16.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
197.135.127.71	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.33.233.116	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
100.100.59.248		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
77.127.193.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
71.30.0.65	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
181.28.167.49	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
176.12.138.149	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
185.69.144.167	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.140.178.82	United States	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	11
37.142.122.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
93.173.43.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
84.108.134.84	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
185.120.126.7		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
100.100.9.106		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
37.142.221.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
2.52.135.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.80.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.98.148.82	Poland	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
176.12.142.87	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
5.22.129.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
198.58.102.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.169.150	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.80.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.12.146.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.32.208.16	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
31.168.218.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.180.31.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
157.55.2.167	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
77.125.127.29	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

10-21-2015-00:04:08 to 10-21-2015-01:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.131	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	78
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	78
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	52
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/size220x0/14570.jpg	Block	13
85.250.41.49	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	13
66.249.67.202	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	13
46.19.85.69	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	13
109.66.80.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	13
79.98.148.82	Poland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
66.249.64.249	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	13
207.46.13.141	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
87.69.241.92	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 87.69.241.92 (Open Mode)	None	13
46.19.85.69	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method 6,en;q=0.4 in URL	Block	13
109.66.80.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	13
87.69.241.92	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	13
54.193.113.160	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	13
109.67.28.165	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	13
84.108.134.84	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	13
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
91.200.13.64	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/wp-load.php	Block	13
66.249.64.151	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/contactus/contactus.aspx	Block	13
176.12.138.149	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	13
84.111.188.182	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/oref/site/he	Block	13
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	13
5.28.130.43	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
109.66.80.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	13
78.148.200.85	United Kingdom	147.237.77.216	dover.idf.il	NULL Character in Method	Block	13
66.249.64.156	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1086-ar/hamaz.aspx	Block	13

10-21-2015-00:04:08 to 10-21-2015-01:04:08