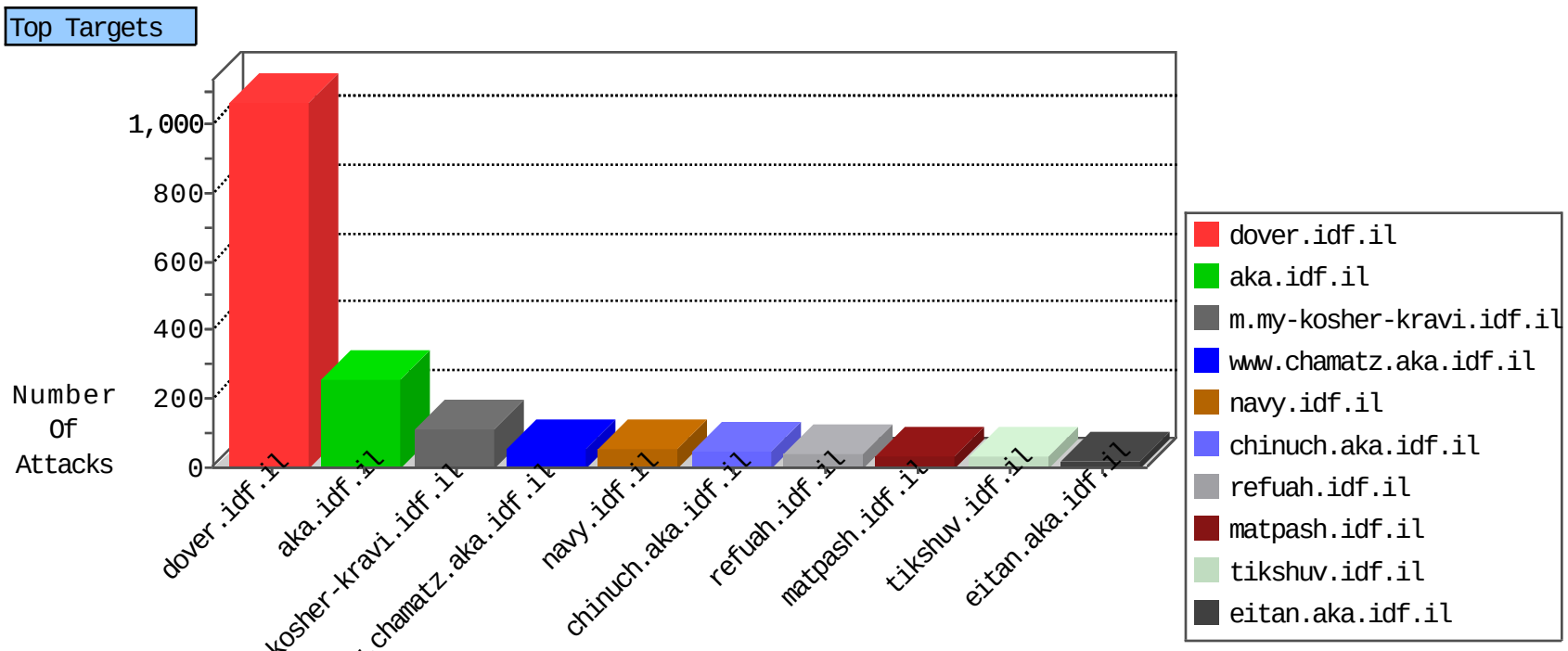
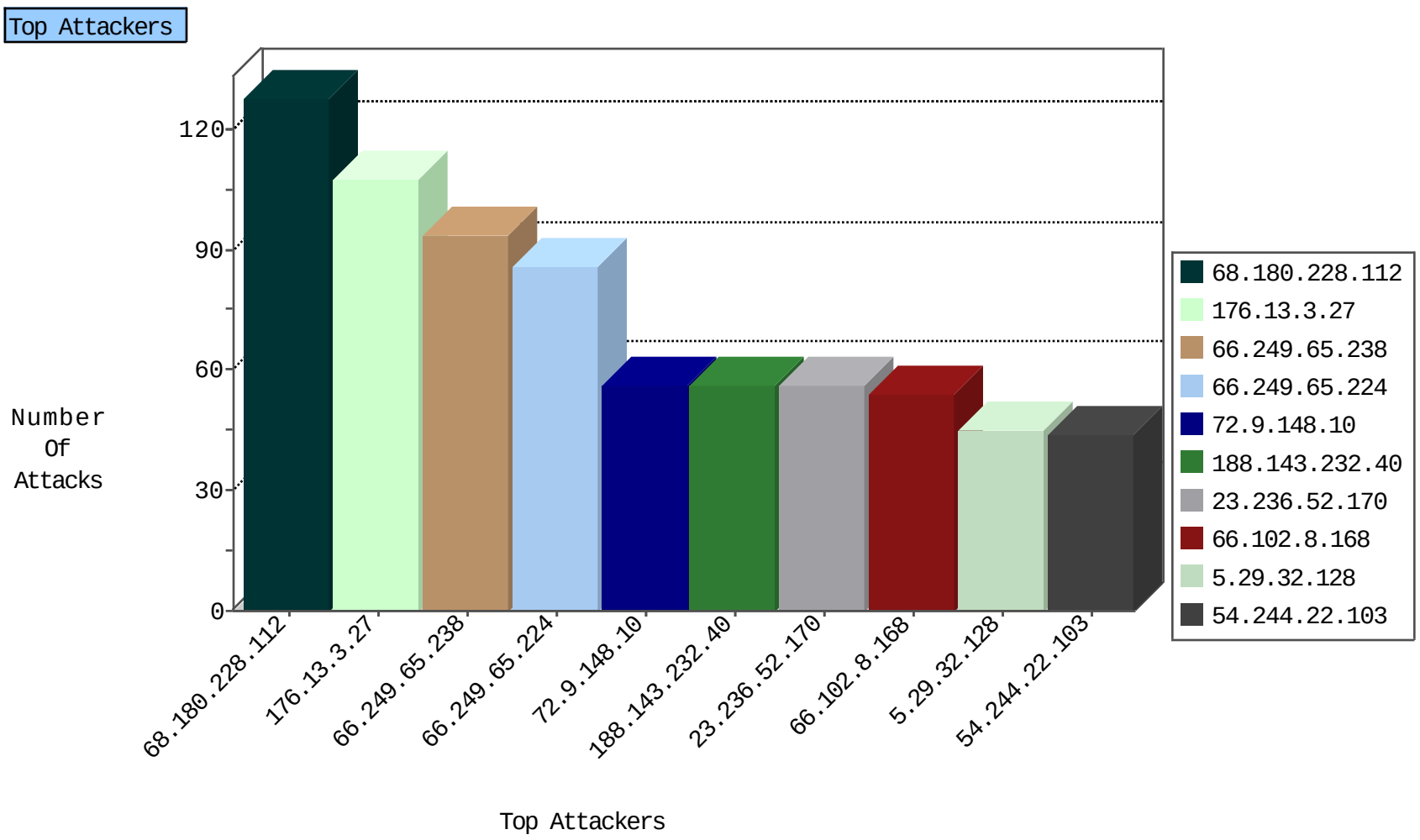
10-24-2015-09:04:01 to 10-24-2015-10:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-24-2015-09:04:01 to 10-24-2015-10:04:01

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	136
31.154.89.50	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	41
5.29.32.128	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	31
84.109.180.11	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
79.183.144.231	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
2.54.187.71	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
85.64.79.170	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
2.54.187.71	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
37.142.215.95	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
2.54.28.24	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
2.54.28.24	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
84.229.134.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
81.218.235.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.187.71	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
85.64.79.170	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
112.198.82.175	Philippines	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
212.143.152.29	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
81.218.234.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
5.102.194.169	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.10.244	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
178.162.203.210	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.141.48	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
109.67.108.232	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.13.22.121	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.86.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
85.250.207.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
213.244.65.90	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
46.121.153.149	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
87.68.30.233	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
79.182.51.32	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
212.143.152.29	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
79.182.51.32	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
5.29.32.128	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
212.143.152.29	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-24-2015-09:04:01 to 10-24-2015-10:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	36
77.126.83.99	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.74.100.10	United States	147.237.77.234	halag.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

10-24-2015-09:04:01 to 10-24-2015-10:04:01

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	3
148.251.180.152	147.237.77.176	Germany	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
196.218.155.73	147.237.77.74	Egypt	law.idf.il	ET SCAN NMAP -sS window 3072	1
185.82.201.17	147.237.77.216		dover.idf.il	ET DOS SSL Bomb DoS Attempt	1
113.229.140.123	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
64.15.155.71	147.237.0.35	Canada	akaws.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
98.158.186.8	147.237.76.176	United States	test.ncore.idf.i	ET SCAN NMAP -sS window 1024	1

10-24-2015-09:04:01 to 10-24-2015-10:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.102.8.168	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
2.54.28.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
100.100.123.190		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
79.183.144.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
2.54.187.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
100.100.75.172		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	14
5.29.32.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
5.22.129.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.140.188.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.22.25.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.160.224.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
197.134.127.111	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.121.153.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.109.180.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.228.110.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
31.210.186.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
203.127.96.199	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.142.225.188	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
31.154.89.50	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
86.14.114.121	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
149.78.230.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.104.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.199.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.134	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
119.73.253.6	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.181.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.108.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.64.79.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.186.143.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
130.0.62.225	Ukraine	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.182.199.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
130.0.62.225	Ukraine	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	4
79.178.108.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
130.0.62.225	Ukraine	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.183.114.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	4
81.218.234.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.3.27	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.3.27	None	94
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	84
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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1781-he/dover.aspx	Block	42
23.236.52.170	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 23.236.52.170	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_img.asp	Block	28
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
188.143.232.40	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 188.143.232.40	Block	28
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	28
2.54.181.79	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	14
188.143.232.40	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	14
81.209.177.189	Europe	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	Unauthorized URL Access to www.idf.il/international_training/catalog.asp	Block	14
203.133.168.29	Korea, Republic of	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
157.55.39.196	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	14
85.65.103.128	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 85.65.103.128 (Open Mode)	None	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
203.133.170.9	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
62.210.88.201	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to 51.254.206.142/httptest.php	Block	14
176.13.3.27	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding UBN1;Eum$N!it5i:Tih	None	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	14
23.236.52.170	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/about	Block	14
188.143.232.40	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1319-he/	Block	14
85.65.103.128	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	14
207.46.13.144	United States	147.237.77.216	dover.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
77.125.151.209	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/chinuch/klali/	None	14
66.249.65.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
54.179.134.216	Singapore	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /	Block	14
192.99.39.235	Canada	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	14
109.66.162.244	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.66.162.244	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
182.118.70.240	China	147.237.0.34	tikshuv.idf.il	URL is Above Root Directory www.tikshuv.idf.il/../shared/clientscripts/jquery/jquery-1.7.1.js	Block	14
79.183.227.92	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	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
195.154.146.225	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-content/	Block	14
54.179.134.216	Singapore	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	14
109.66.162.244	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	14

10-24-2015-09:04:01 to 10-24-2015-10:04:01