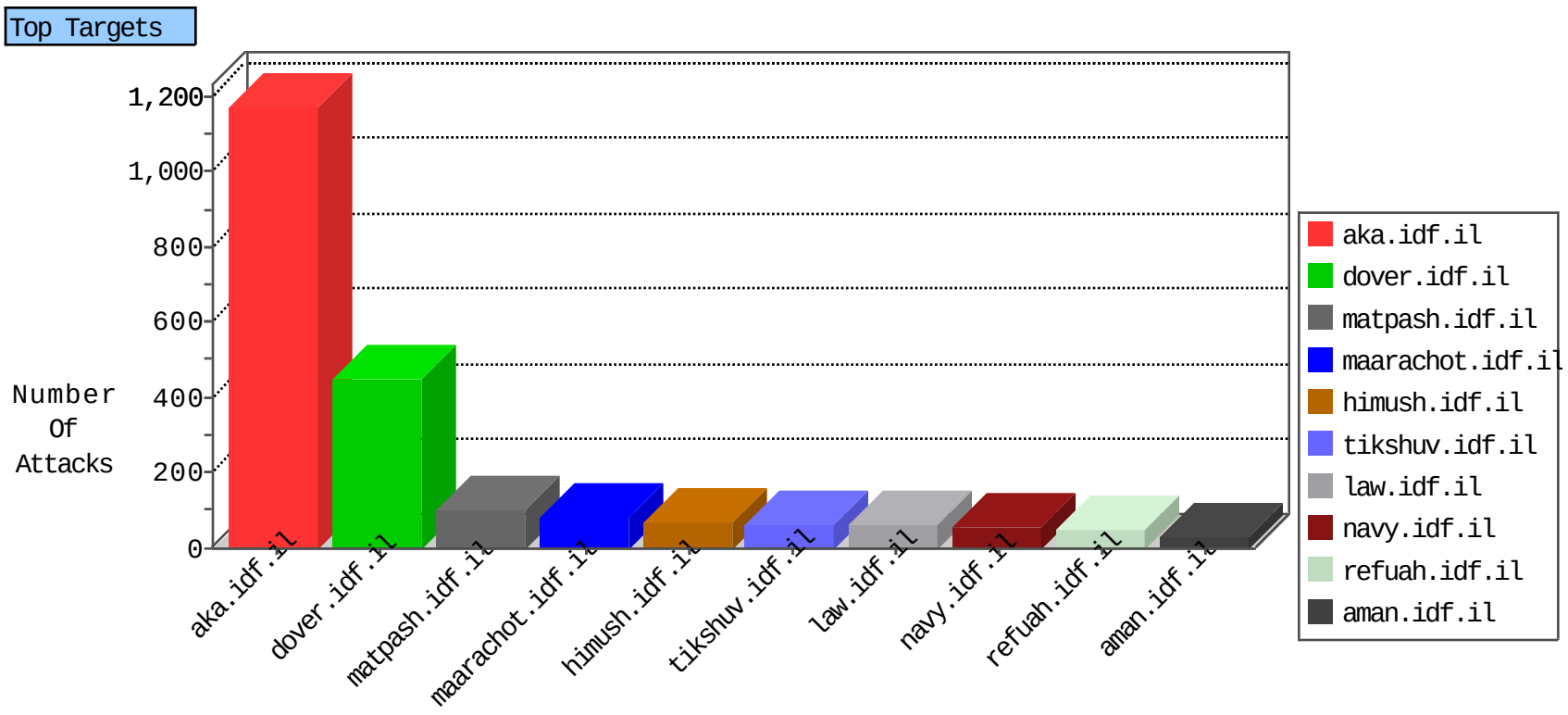
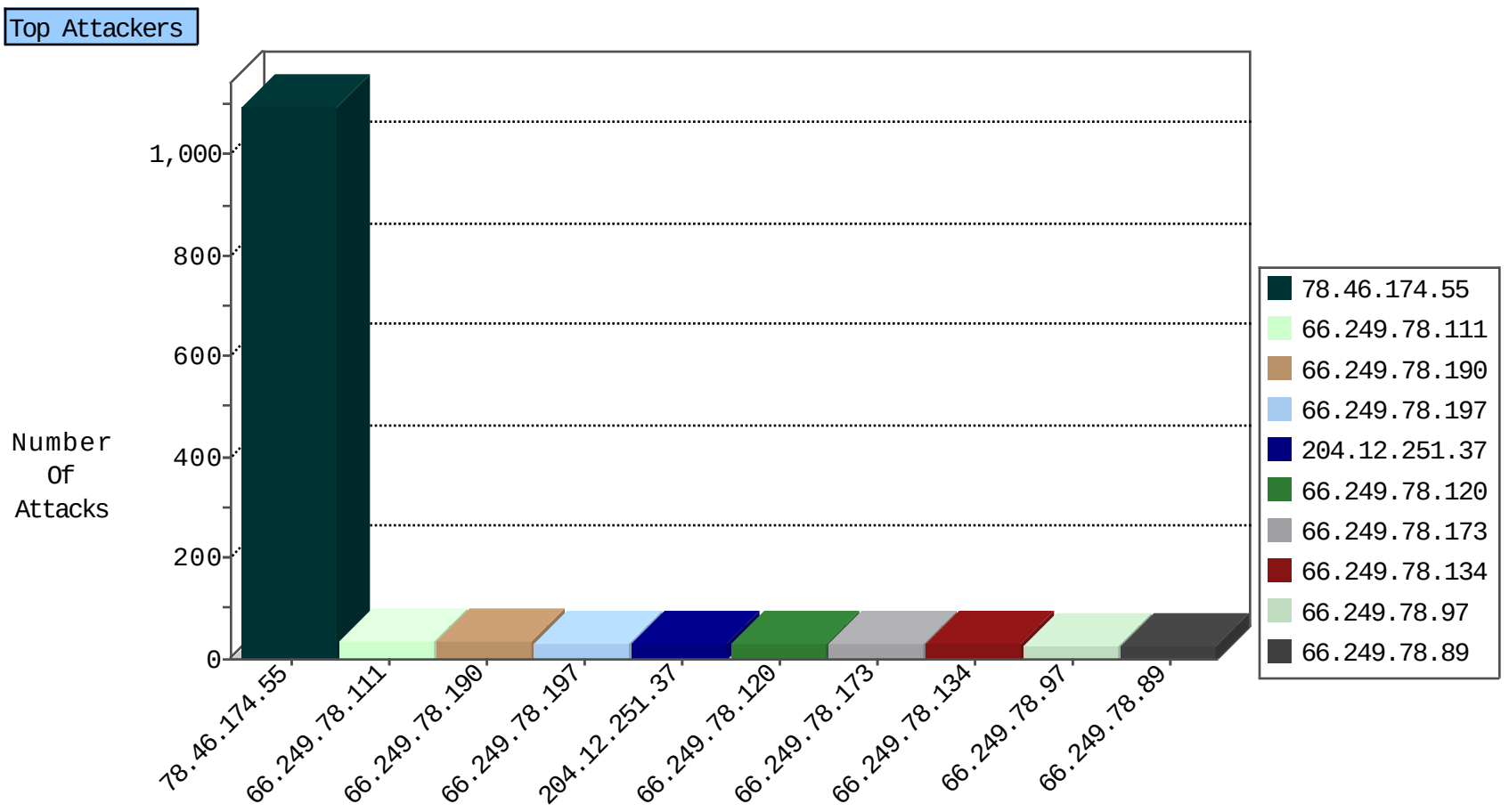
04-10-2015-04:03:00 to 04-10-2015-05:03:00

IDF Under Attack
04-10-2015-04:03:00

Top Targets



Top Attackers



04-10-2015-04:03:00 to 04-10-2015-05:03:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.187	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	366
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	34
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	33
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	31
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	29
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	28
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	28
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	27
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	26
66.249.65.155	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	26
66.249.65.151	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	25
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	25
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	23
66.249.65.147	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	18
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	18
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	17
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	16
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	16
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	14
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	14
66.249.69.8	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	13
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.64.147	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	12
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.80.83	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.89.101	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
66.249.65.186	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	7
66.249.64.63	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	6
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.249.67.3	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.65.132	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	6
66.249.78.15	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	5
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	5
66.249.67.155	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
66.249.65.178	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	5
66.249.64.146	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
66.249.81.207	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	4
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
66.249.78.22	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	4
66.249.81.209	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
66.249.64.151	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	4
66.249.81.212	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	3
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	3

04-10-2015-04:03:00 to 04-10-2015-05:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
93.120.27.62	Romania	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
192.67.133.200	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-10-2015-04:03:00 to 04-10-2015-05:03:00

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
43.255.191.141	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
209.126.230.72	United States	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.141	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
177.85.235.107	Brazil	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.141	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
94.131.14.10	Russian Federation	147.237.77.74	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
43.255.191.141	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.231	Netherlands	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.141	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
213.136.84.245	Germany	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.141	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
174.226.194.155	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.141	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.231	Netherlands	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

04-10-2015-04:03:00 to 04-10-2015-05:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
31.168.71.97	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
46.19.85.185	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
204.12.251.37	United States	147.237.0.15	kosher-kravi.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	20
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
76.219.190.87	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
50.51.82.104	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
79.181.113.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
185.11.11.242	Yemen	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
85.64.151.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
185.23.127.21	Bahrain	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
194.187.168.26	Poland	147.237.77.176	matpash.idf.il	SAM rule	drop	drop	6
93.168.255.74	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
108.82.173.237	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
81.218.80.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
174.226.194.155	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
110.142.129.112	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
204.237.22.235	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
190.156.104.191	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
99.235.104.105	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
104.162.241.87		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.114	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
204.12.251.37	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.65.43.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.135.76.178	Czech Republic	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
198.58.103.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
151.203.67.34	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.139.52.36	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
5.29.104.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
220.255.1.139	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
24.29.224.88	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
75.147.181.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
5.29.248.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

04-10-2015-04:03:00 to 04-10-2015-05:03:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.46.174.55	Block	437
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 78.46.174.55	Block	301
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 78.46.174.55	Block	301
204.12.251.37	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/'	Block	2
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	2
204.12.251.37	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	2
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
190.107.176.148	Chile	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/×ª/main/giyus	Block	1
157.55.39.130	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Illegal HTTP Version ×″×—×™× ×•×š ×•×″× ×• ×¢×¨&body=http://www.aka.idf.il/chinuch/home/default.asp?catId=42142&docId= HTTP/1.1	Block	1
5.79.16.135	United Kingdom	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
192.67.133.200	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/navy/service.stm	Block	1
94.159.160.107	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00_ctl00_ScriptManager1_HiddenField in www.aka.idf.il/main/sachar/	None	1
74.82.47.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
204.12.251.37	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
188.40.28.160	Germany	147.237.77.216	dover.idf.il	Extremely Long HTTP Request	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
203.217.64.68	Australia	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
104.131.210.158		147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
74.112.131.246	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-220	Block	1
209.126.230.72	United States	147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_SERVER_HELLO)	None	1
188.40.28.160	Germany	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method	Block	1
37.140.141.27	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
204.12.251.37	United States	147.237.0.15	kosher-kravi.idf.il	URL is Above Root Directory www.kosher-kravi.idf.il/../shared/usercontrols/headerupper/	Block	1
155.94.222.12		147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Abnormally Long Request request version	Block	1
209.126.230.72	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 209.126.230.72 (Protocol violation (SSL_CONN_SERVER_HELLO))	None	1
189.212.234.209	Mexico	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1

04-10-2015-04:03:00 to 04-10-2015-05:03:00