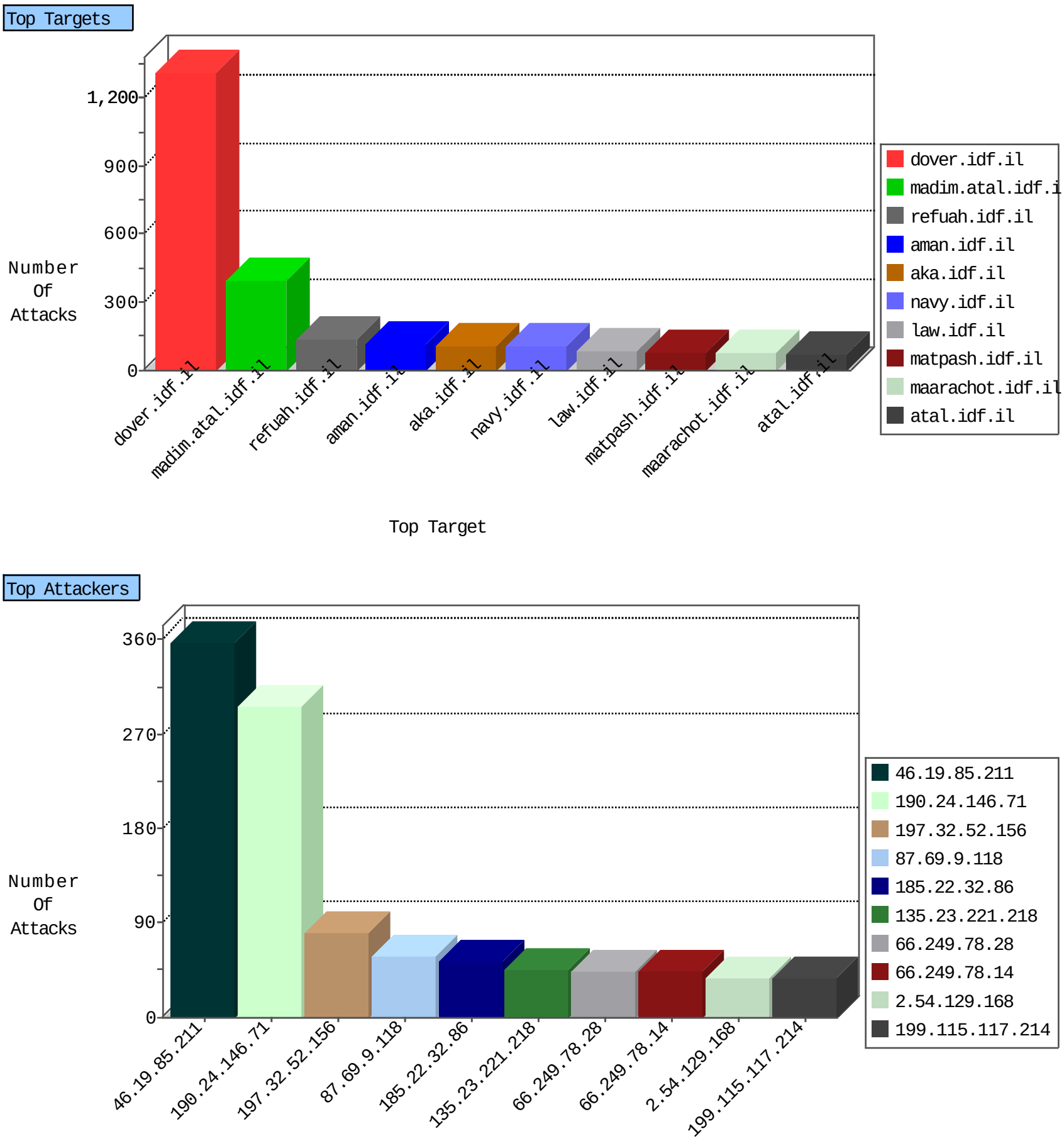
04-10-2015-01:03:05 to 04-10-2015-02:03:05

IDF Under Attack
04-10-2015-01:03:05



04-10-2015-01:03:05 to 04-10-2015-02:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
87.69.9.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	819
220.181.108.123	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	398
185.22.32.86	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	382
84.108.81.124	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	311
79.180.194.164	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	113
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	44
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	44
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	37
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	35
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	33
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	33
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	32
66.249.67.30	United States	147.237.76.86	navy.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
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	27
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	26
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	23
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	22
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	21
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	21
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	18
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	18
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	16
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	15
66.249.69.34	United States	147.237.72.166	aka.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
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.69.105	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	9
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.78.29	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.69.113	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	9
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	9
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.78.67	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.78.22	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	7
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.69.97	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	7
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.89.103	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.80.127	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.64.55	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	6
66.249.64.41	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	6
66.249.64.151	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	5
66.249.89.105	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	5
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	4

04-10-2015-01:03:05 to 04-10-2015-02:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	5
93.120.27.62	Romania	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
79.183.35.92	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.8.27	e.madim.atal.idf.i	DVRep_B-N_60_100	Block	1

04-10-2015-01:03:05 to 04-10-2015-02:03:05

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	5
91.224.132.118	Russian Federation	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
8.29.144.205	United States	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
8.29.144.205	United States	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
151.236.58.222	United Kingdom	147.237.77.216	dover.idf.il	POLICY-OTHER Adobe ColdFusion admin interface access attempt	1
113.21.226.56	New Zealand	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	Turkey	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
8.29.144.205	United States	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
151.236.58.222	United Kingdom	147.237.77.216	dover.idf.il	ET WEB_SERVER ColdFusion administrator access	1

04-10-2015-01:03:05 to 04-10-2015-02:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
190.24.146.71	Colombia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	290
197.32.52.156	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	80
185.22.32.86	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
135.23.221.218	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
199.115.117.214	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
88.235.250.157	Turkey	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
109.160.134.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
176.12.138.23	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
176.12.138.26	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
2.115.17.164	Italy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
62.90.184.90	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
46.19.85.103	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
109.253.128.168	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
82.145.222.216	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
188.48.243.211	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
109.65.177.231	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
64.233.173.156	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
50.41.213.233	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
89.139.185.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
5.57.242.191	Sweden	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
84.94.155.30	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
109.253.137.146	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
199.119.233.154	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
178.153.81.31	Qatar	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
166.137.244.119	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
109.253.143.252	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
188.40.28.160	Germany	147.237.77.216	dover.idf.i	Response out of state	Block HTTP Non Compliant	monitor	8
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
74.83.98.90	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
46.19.85.121	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
87.68.57.239	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
99.149.20.22	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
213.57.112.93	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
190.24.146.71	Colombia	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	6
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
190.255.39.202	Colombia	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	5
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
190.255.39.202	Colombia	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	5
157.55.39.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
46.19.85.170	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	5
197.135.127.226	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
157.55.39.114	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
188.40.28.160	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
192.241.245.200	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
79.179.125.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4

04-10-2015-01:03:05 to 04-10-2015-02:03:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	358
2.54.129.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	38
188.40.28.160	Germany	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	8
188.40.28.160	Germany	147.237.77.216	dover.idf.il	Distributed Extremely Long HTTP Request	Block	7
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	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
81.31.35.48	Czech Republic	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
157.55.39.101	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14363-he/dover.aspx	Block	1
79.182.126.85	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
198.170.241.46	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
84.228.140.106	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.172	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
162.243.202.56	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
79.183.35.92	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
109.253.143.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.67.28.130	Germany	147.237.77.216	dover.idf.il	Distributed Extremely Long HTTP Request	Block	1
5.39.85.41	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
134.0.11.76	Spain	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
80.67.28.130	Germany	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
37.59.29.19	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
75.119.222.136	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
188.40.28.160	Germany	147.237.77.216	dover.idf.il	Multiple Extremely Long HTTP Request from 188.40.28.160	Block	1

04-10-2015-01:03:05 to 04-10-2015-02:03:05