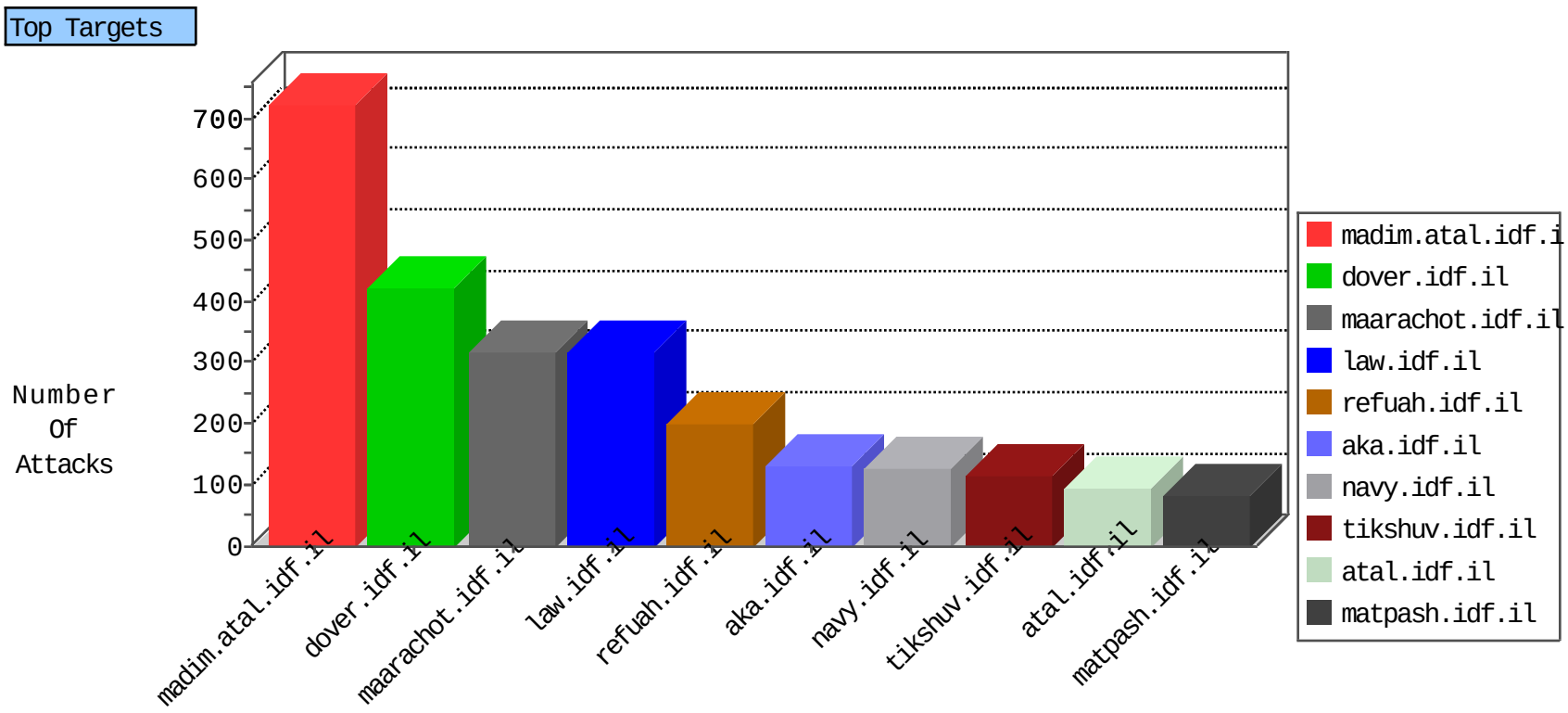
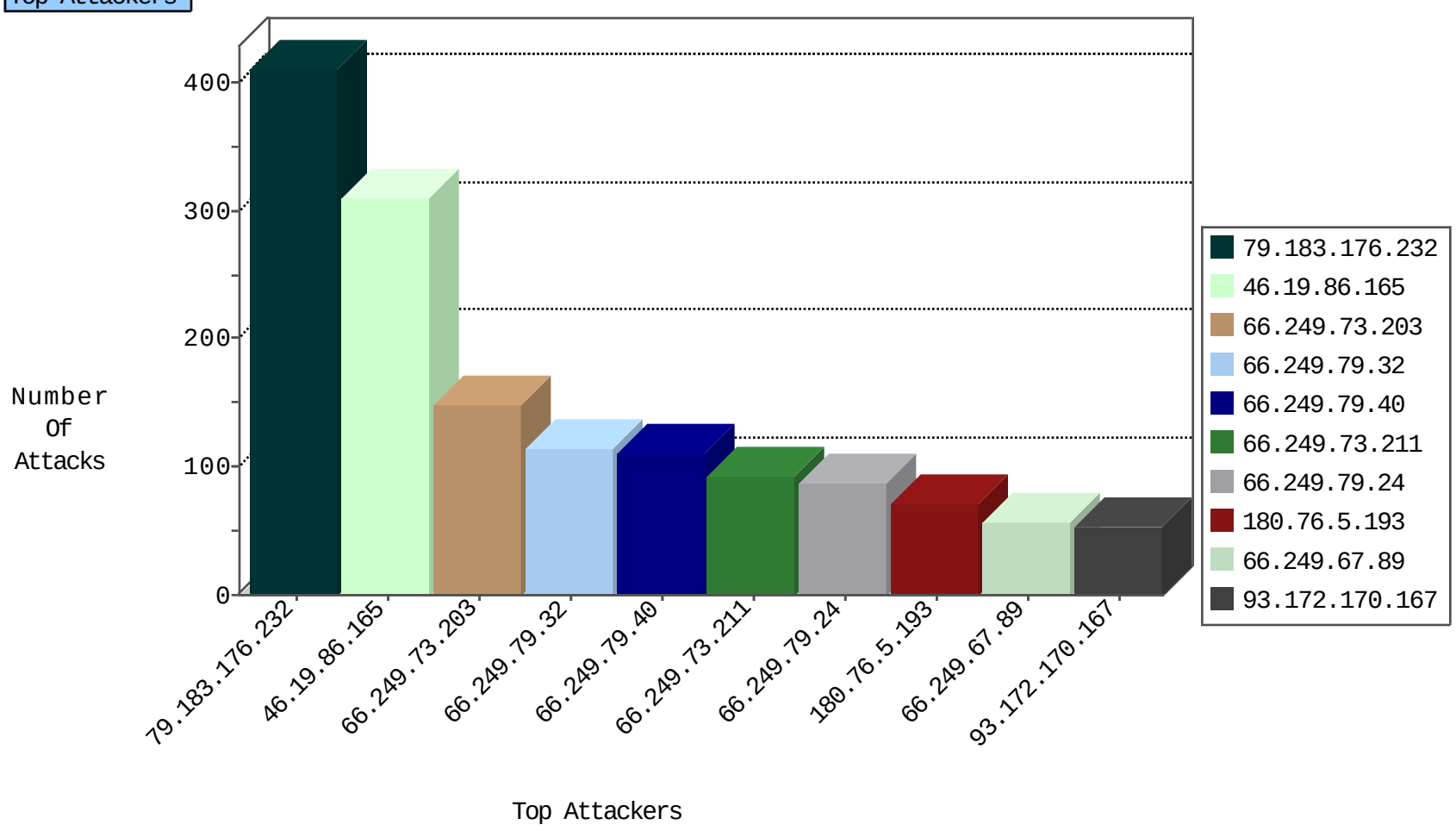
04-06-2015-01:03:01 to 04-06-2015-02:03:01

IDF Under Attack
04-06-2015-01:03:01

Top Targets



Top Attackers



04-06-2015-01:03:01 to 04-06-2015-02:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
79.176.158.232	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
66.249.73.203	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	147
66.249.79.32	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	113
66.249.79.40	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	110
66.249.73.211	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	92
66.249.79.24	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	87
66.249.67.89	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	55
66.249.67.73	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	53
66.249.73.219	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	53
66.249.67.81	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	48
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	36
66.249.65.199	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	35
66.249.65.191	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	32
66.249.65.195	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	31
66.249.65.132	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	30
66.249.78.154	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	30
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	28
66.249.73.129	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	26
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	25
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	25
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	24
66.249.78.130	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	23
66.249.78.144	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	23
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	22
66.249.78.147	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	21
66.249.67.29	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	21
66.249.79.34	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	19
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	19
66.249.79.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	19
66.249.78.161	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	17
66.249.81.212	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	16
66.249.79.50	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	16
66.249.79.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	14
66.249.79.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.73.187	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.73.195	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.73.241	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.73.233	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.79.13	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.79.5	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.81.215	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.65.135	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	8
66.249.92.63	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.65.136	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	7
66.249.79.157	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.79.42	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.137	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	7
66.249.81.218	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7

04-06-2015-01:03:01 to 04-06-2015-02:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	71
84.109.197.191	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
93.172.170.167	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.69.98	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1

04-06-2015-01:03:01 to 04-06-2015-02:03:01

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
61.240.144.67	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
41.251.199.122	Morocco	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.212	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
181.143.135.66	Colombia	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
177.129.79.177	Brazil	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
171.111.158.207	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
198.51.75.164	Canada	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
181.143.135.66	Colombia	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
177.129.79.177	Brazil	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
177.129.79.177	Brazil	147.237.77.205	prisha.idf.il	ET SCAN NMAP -f -sS	1
221.235.188.212	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
171.111.158.207	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1

04-06-2015-01:03:01 to 04-06-2015-02:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.109.197.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
93.172.170.167	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	28
109.253.141.183	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
93.172.170.167	Israel	147.237.72.166	aka.idf.il	SAM rule	drop	drop	11
109.253.138.1	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	6
199.30.25.196	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	6
176.12.139.246	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
93.172.170.167	Israel	147.237.72.166	aka.idf.il		drop	drop	5
8.37.228.77	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	5
37.247.36.106	Netherlands	147.237.76.197	e.himush.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	5
93.172.170.167	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	4
41.203.67.161	Nigeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
70.39.187.112	Satellite Provide	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	3
105.210.180.197	South Africa	147.237.77.216	dover.idf.il	SAM rule	drop	drop	2
8.37.228.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	2
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
50.7.71.91	United States	147.237.76.44	e.refuah.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
157.55.39.66	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
70.39.186.218	Satellite Provide	147.237.77.233	atal.idf.il	Response out of state	Block HTTP Non Compliant	monitor	2
80.246.130.157	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.50	United States	147.237.76.197	e.himush.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
70.39.186.222	Satellite Provide	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
188.138.17.205	France	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.57	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.56	United States	147.237.76.147	chinuch.aka.idf.il		drop	drop	1
70.39.187.108	Satellite Provide	147.237.77.233	atal.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
141.212.122.57	United States	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.121.163	United States	147.237.76.34	yohalan.idf.il		drop	drop	1
84.110.216.1	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	1
8.37.227.70	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
70.39.187.112	Satellite Provide	147.237.77.233	atal.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
141.212.121.165	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
84.110.216.1	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	1

04-06-2015-01:03:01 to 04-06-2015-02:03:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.183.176.232	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.183.176.232	Block	411
46.19.86.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	310
5.28.130.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	3
188.165.15.198	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.198	Block	3
5.29.120.251	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
176.57.143.60	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.138.75.23	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.119.189	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.198	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
109.186.9.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/updateuserdetails.aspx	Block	1
79.183.119.248	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
216.218.207.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
178.155.164.7	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
91.216.241.78	Ireland	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
109.253.129.92	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
79.183.176.232	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
218.232.75.133	Korea, Republic of	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
5.28.163.234	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
184.168.200.180	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
93.173.30.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal/uzi-levtzur-h.stm	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
203.133.169.157	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/phones.stm	Block	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	1
188.93.144.48	Netherlands	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
94.23.54.167	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
70.167.8.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluimtemplates/inner.asp	Block	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
157.55.39.66	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.110.216.1	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
188.138.17.205	France	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
109.67.203.179	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.241.226.125	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1

04-06-2015-01:03:01 to 04-06-2015-02:03:01