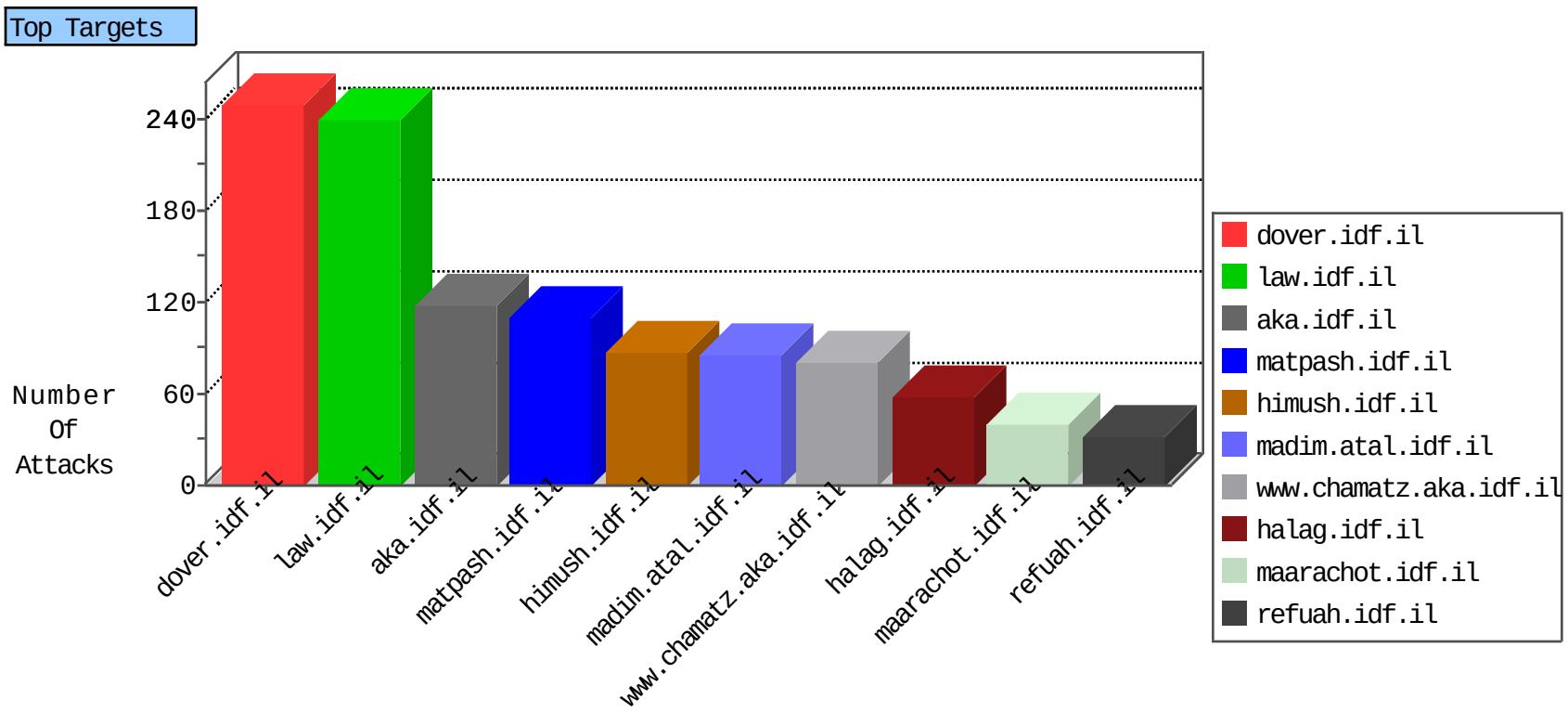
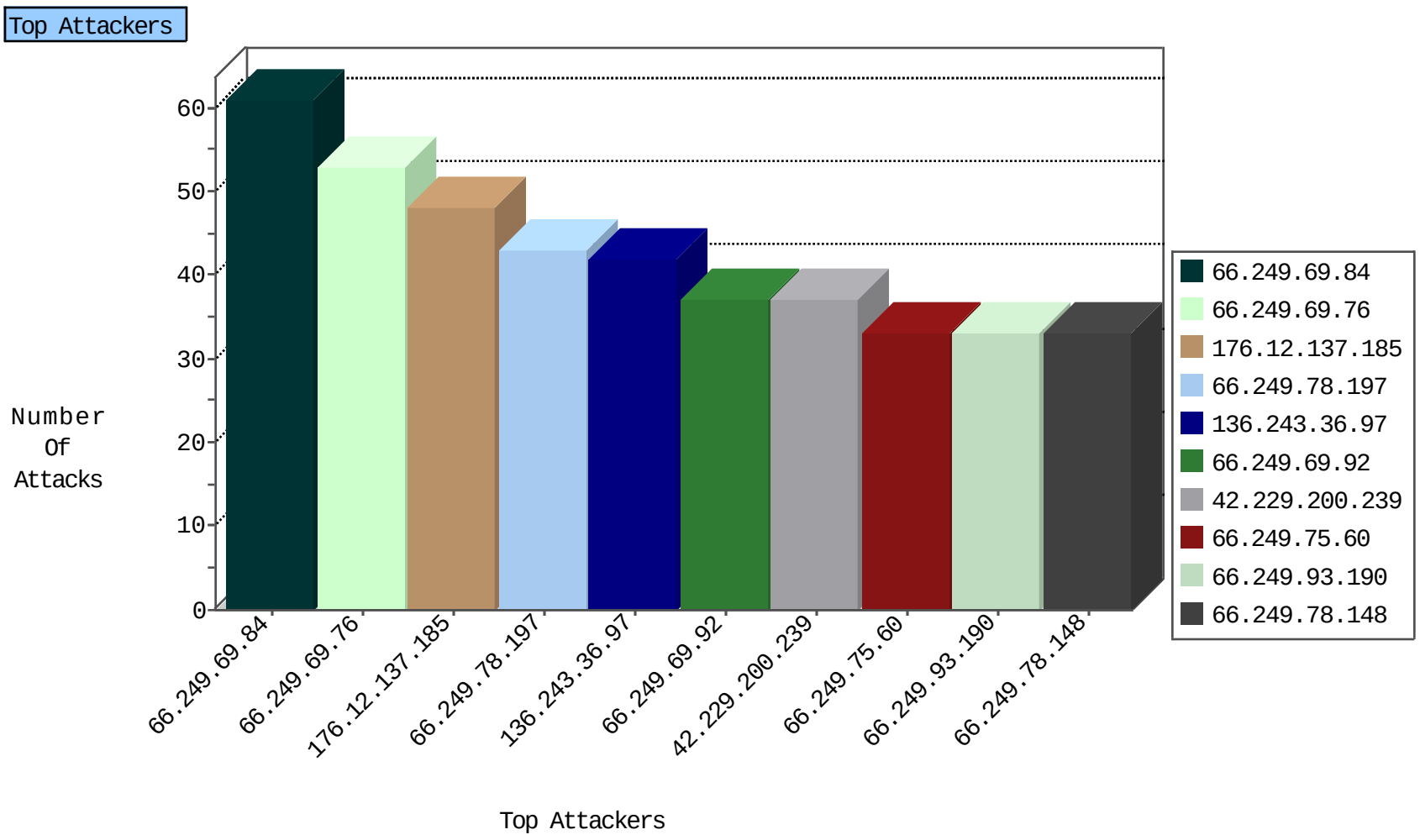
04-03-2015-21:03:05 to 04-03-2015-22:03:05

IDF Under Attack
04-03-2015-21:03:05





04-03-2015-21:03:05 to 04-03-2015-22:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.69.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	61
66.249.69.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	53
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	43
66.249.69.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	37
66.249.75.60	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	33
66.249.78.148	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	33
66.249.93.190	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	33
66.249.75.68	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	31
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	30
66.249.78.141	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	26
66.249.78.134	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	25
66.249.93.240	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	24
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	23
66.249.93.186	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	23
66.249.93.243	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	21
66.249.93.194	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	20
66.249.93.237	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	20
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	17
66.249.75.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	17
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.67.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.67.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	14
66.249.78.191	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	12
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	12
66.249.78.38	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	12
66.249.80.67	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.67.13	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.75.111	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	9
66.249.67.157	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	7
66.249.64.114	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	7
66.249.67.5	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.64.118	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.67.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.84.182	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.64.110	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.69.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.78.228	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	5
66.249.92.51	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	5
66.249.64.49	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	4
66.249.67.138	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	4
66.249.78.31	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	4

04-03-2015-21:03:05 to 04-03-2015-22:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
42.229.200.239	China	147.237.77.170	maarachot.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
42.229.200.239	China	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
204.75.207.117	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
89.139.182.210	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
197.176.96.254	Kenya	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.103.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	2
85.25.103.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	2
85.25.103.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
188.161.114.49	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.183.51.248	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.176	test.ncore.idf.i	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old	DVRep_B-N_60_100	Block	1

04-03-2015-21:03:05 to 04-03-2015-22:03:05

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
37.26.146.198	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.66	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
27.50.132.61	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.66	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
59.41.39.125	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 4096	1
188.138.9.51	Germany	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.168	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
183.232.116.154	China	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.168	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
173.33.214.118	Canada	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.168	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
109.104.79.112	United Kingdom	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
85.194.93.41	Saudi Arabia	147.237.76.202	e.halag.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
43.255.191.168	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.176	matpash.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
27.50.132.61	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.66	China	147.237.76.39	mobile.meitav.idf.i	ET SCAN Potential VNC Scan 5800-5820	1
27.50.132.61	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.66	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
188.138.9.51	Germany	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
59.41.39.125	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
183.232.116.154	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.168	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
183.232.116.154	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.168	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
114.255.149.210	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
109.104.79.112	United Kingdom	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1

04-03-2015-21:03:05 to 04-03-2015-22:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
176.12.137.185	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
136.243.36.97	Germany	147.237.77.216	dover.idf.il	SAM rule	drop	drop	42
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	30
109.253.144.199	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
176.12.144.214	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.132.131	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.135.121	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.28.142.41	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.85.142	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
188.120.148.210	Israel	147.237.76.39	mobile.meitav.idf.i	Invalid ACK number	Bad TCP sequence	monitor	3
98.143.148.107	United States	147.237.76.147	chinuch.aka.idf.il		drop	drop	2
185.20.4.220	United Kingdom	147.237.77.170	maarachot.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.186	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
37.16.72.139	France	147.237.0.15	kosher-kravi.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.86.151	Israel	147.237.0.19	madim.atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
196.217.34.133	Morocco	147.237.77.216	dover.idf.il		drop	drop	2
46.19.86.152	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
198.20.69.74	United States	147.237.0.33	idf.il	SAM rule	drop	drop	1
141.212.122.72	United States	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
79.178.161.133	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
218.22.211.69	China	147.237.76.44	e.refuah.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.173	United States	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.61	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.227	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.192	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
86.111.149.194	Iraq	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.96	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
188.120.148.210	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
88.150.252.33	United Kingdom	147.237.0.33	idf.il		drop	drop	1
5.9.97.92	Germany	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
79.178.161.133	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1

04-03-2015-21:03:05 to 04-03-2015-22:03:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
42.229.200.239	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 42.229.200.239	Block	3
42.229.200.239	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 42.229.200.239	Block	3
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
94.23.30.222	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
79.183.51.248	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
42.229.200.239	China	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	2
176.12.136.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	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
167.114.64.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
79.181.139.103	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
42.229.200.239	China	147.237.77.170	maarachot.idf.il	CVE-2008-7212: Mambo 4.6.3 Path Disclosure Vulnerability	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/history/degania.stm	Block	1
42.229.200.239	China	147.237.72.166	aka.idf.il	Multiple CVE-2008-7212: Mambo 4.6.3 Path Disclosure Vulnerability(+) from 42.229.200.239	Block	1
175.42.91.134	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/7/3317.pdf/trackback/	Block	1
203.133.169.157	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
109.253.130.211	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
70.167.8.42	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-en/patzar.aspx	Block	1
89.248.171.167	Netherlands	147.237.76.39	mobile.meitav.idf.i	Unauthorized URL Access to 147.237.76.39/wp-content/plugins/simple-ads-manager/	Block	1
42.229.200.239	China	147.237.77.170	maarachot.idf.il	Multiple CVE-2008-7212: Mambo 4.6.3 Path Disclosure Vulnerability(+) from 42.229.200.239	Block	1
149.78.38.216	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
42.229.200.239	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
89.248.171.167	Netherlands	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/wp-content/plugins/simple-ads-manager/	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
157.55.39.103	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//	Block	1
77.125.121.187	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
42.229.200.239	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/editor/editor/filemanager/connectors/aspx/connector.aspx	Block	1
180.76.4.49	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
93.173.162.90	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
37.59.29.19	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1

04-03-2015-21:03:05 to 04-03-2015-22:03:05