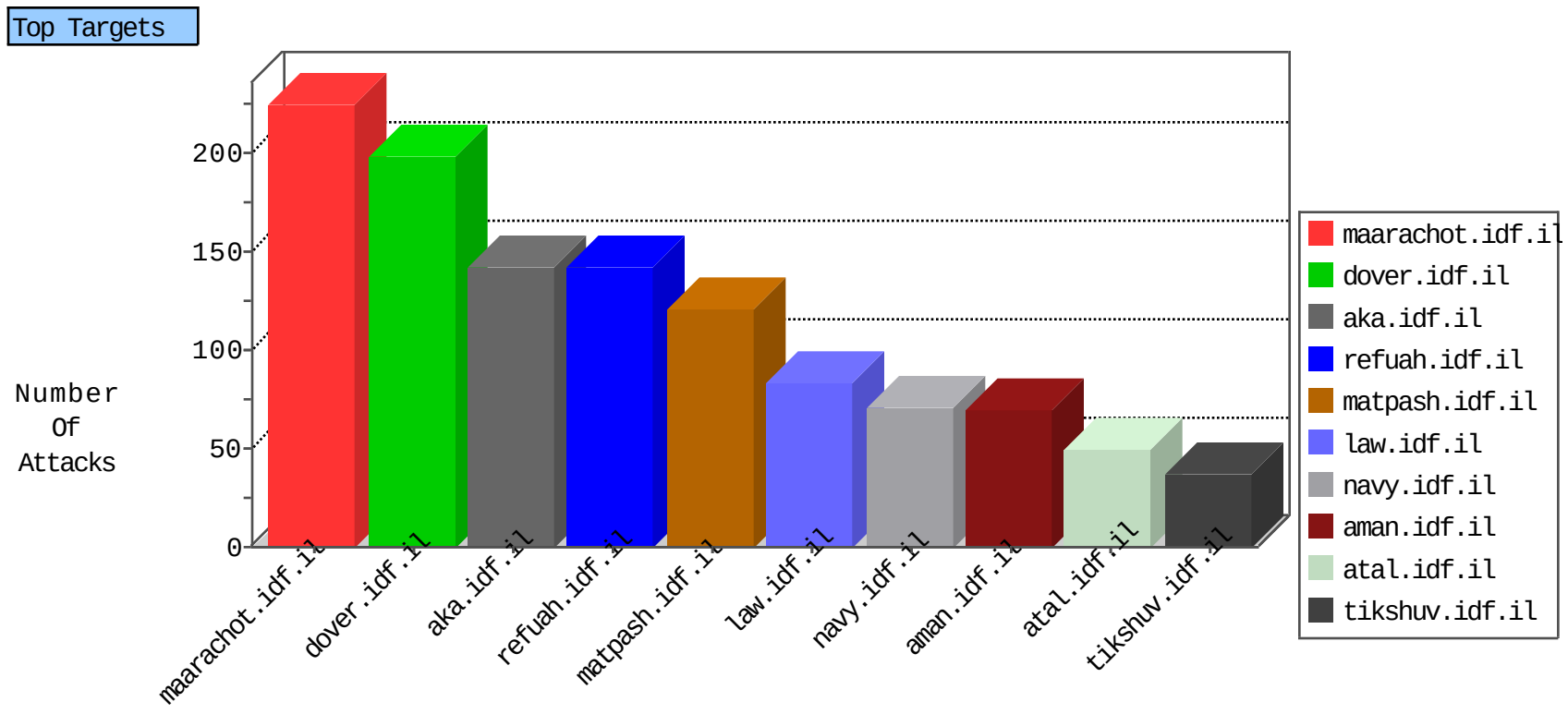
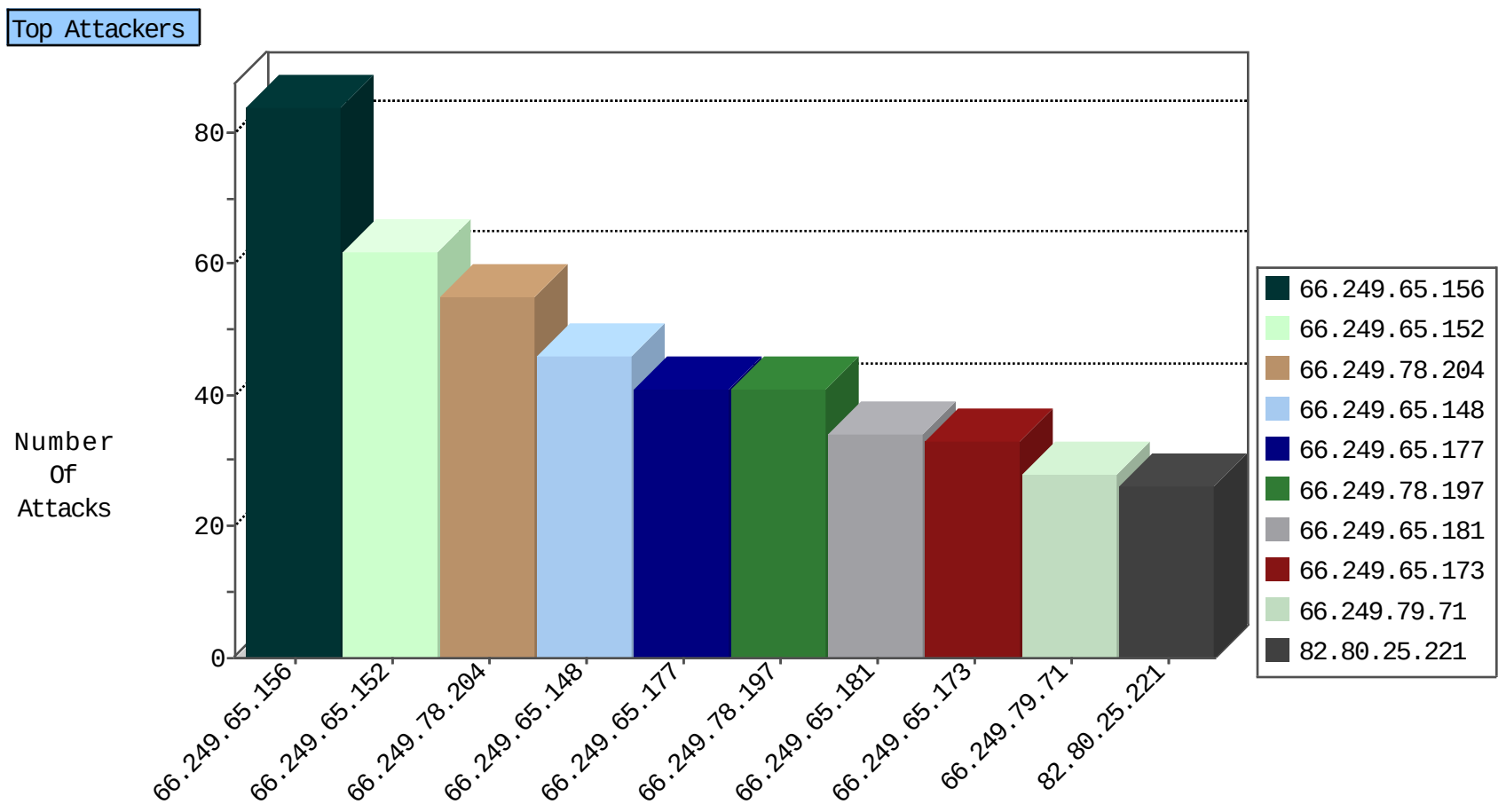
04-05-2015-02:03:01 to 04-05-2015-03:03:01

IDF Under Attack
04-05-2015-02:03:01

Top Targets



Top Attackers



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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	84
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	62
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	55
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	46
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	41
66.249.65.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	41
66.249.65.181	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	34
66.249.65.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	33
66.249.79.71	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	28
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	26
66.249.78.153	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	24
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	22
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	21
66.249.78.144	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	19
66.249.79.63	United States	147.237.72.156	aman.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
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	18
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	18
66.249.78.137	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	18
66.249.65.169	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
66.249.79.42	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	12
66.249.79.55	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	12
66.249.78.141	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	11
66.249.79.34	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.90.90	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	10
66.249.81.144	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.78.130	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
66.249.78.154	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	9
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	9
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.78.47	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	8
66.249.78.146	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.90.82	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	7
66.249.79.124	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	7
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	7
66.249.67.34	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	6
66.249.81.140	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.249.69.99	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	6
66.249.75.23	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	6
66.249.78.228	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	6
66.249.92.63	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.73.136	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	5
66.249.78.148	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	5
66.249.78.134	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	5
66.249.78.222	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	5

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
178.217.187.39	Poland	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	2
162.247.72.200		147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
5.135.148.171	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
173.254.216.66	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
84.228.224.133	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
193.111.136.164	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.34	yohalan.idf.il	DVRep_P-N_40-59	Permit	1
146.185.135.43	Netherlands	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1

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

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
2.54.39.213	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.102.50.40	Netherlands	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
94.102.50.40	Netherlands	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
94.102.50.40	Netherlands	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
176.12.146.208	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.105.45.117		147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.50.40	Netherlands	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
77.105.45.117		147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
94.102.50.40	Netherlands	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.50.40	Netherlands	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.50.40	Netherlands	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
94.102.50.40	Netherlands	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
119.97.231.102	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
89.248.162.228	Netherlands	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.50.40	Netherlands	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
77.105.45.117		147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.50.40	Netherlands	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
69.12.92.160	United States	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
94.102.50.40	Netherlands	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
94.102.50.40	Netherlands	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
94.102.50.40	Netherlands	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
94.102.50.40	Netherlands	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
94.102.50.40	Netherlands	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
119.97.231.102	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	26
109.253.145.76	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.144.50	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
46.19.85.207	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	13
109.253.157.166	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.148.77	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.253.138.130	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.139.253	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
188.120.148.190	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
83.0.160.62	Poland	147.237.72.217	e.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
31.210.186.130	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
98.143.148.107	United States	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
83.0.160.62	Poland	147.237.72.167	ishurim.aka.idf.il	SAM rule	drop	drop	2
109.253.135.11	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.85.92	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
84.228.224.133	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	2
83.0.160.62	Poland	147.237.72.156	aman.idf.il	SAM rule	drop	drop	2
188.120.148.190	Israel	147.237.76.39	mobile.meitav.idf.i	Invalid ACK number	Bad TCP sequence	monitor	2
109.253.133.241	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
61.135.190.198	China	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
98.143.148.107	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
83.0.160.62	Poland	147.237.72.166	aka.idf.il	SAM rule	drop	drop	2
109.253.134.248	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
188.138.1.229	Germany	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
46.19.85.69	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
88.150.187.210	United Kingdom	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
5.199.130.188	Germany	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
109.163.234.2	Romania	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
188.138.9.49	Germany	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
112.111.188.109	China	147.237.77.216	dover.idf.il	SAM rule	drop	drop	1
109.253.135.66	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
94.242.246.23	Luxembourg	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
176.126.252.12	Romania	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
18.243.0.30	United States	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
109.163.234.8	Romania	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
188.138.17.205	France	147.237.76.202	e.halag.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.96	United States	147.237.76.201	e.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
109.253.135.66	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
94.242.252.41	Luxembourg	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
85.130.137.247	Israel	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	1
141.212.122.96	United States	147.237.77.121	e.navy.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
109.253.138.130	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
37.187.129.166	France	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
85.130.137.247	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
62.210.170.27	France	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
141.212.122.161	United States	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
109.253.138.130	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.28.155.175	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	4
216.244.83.168	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.aspx	Block	3
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
188.120.148.190	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	2
188.165.15.238	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9234-he/refuah.aspx	Block	1
94.185.82.114	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-10578-en/dover.aspx/rk=0/rs=dzechxwm6_p05zzu8ghf4clfjj0-	Block	1
70.167.8.42	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/14-he/	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.130.245.242	Israel	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/newsite/english/010804-1.stm	Block	1
95.86.121.3	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	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
87.69.0.196	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	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
213.251.182.10	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	1
109.186.225.69	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
87.69.148.215	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm&	Block	1
115.25.81.73	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
79.181.62.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
188.165.15.198	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.198	Block	1
87.69.148.215	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$btnSubmit.y in www.aka.idf.il/main/sachar/	None	1
46.19.123.125	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//templates/shared/usercontrols/headerupper/	Block	1
84.228.224.133	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1

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