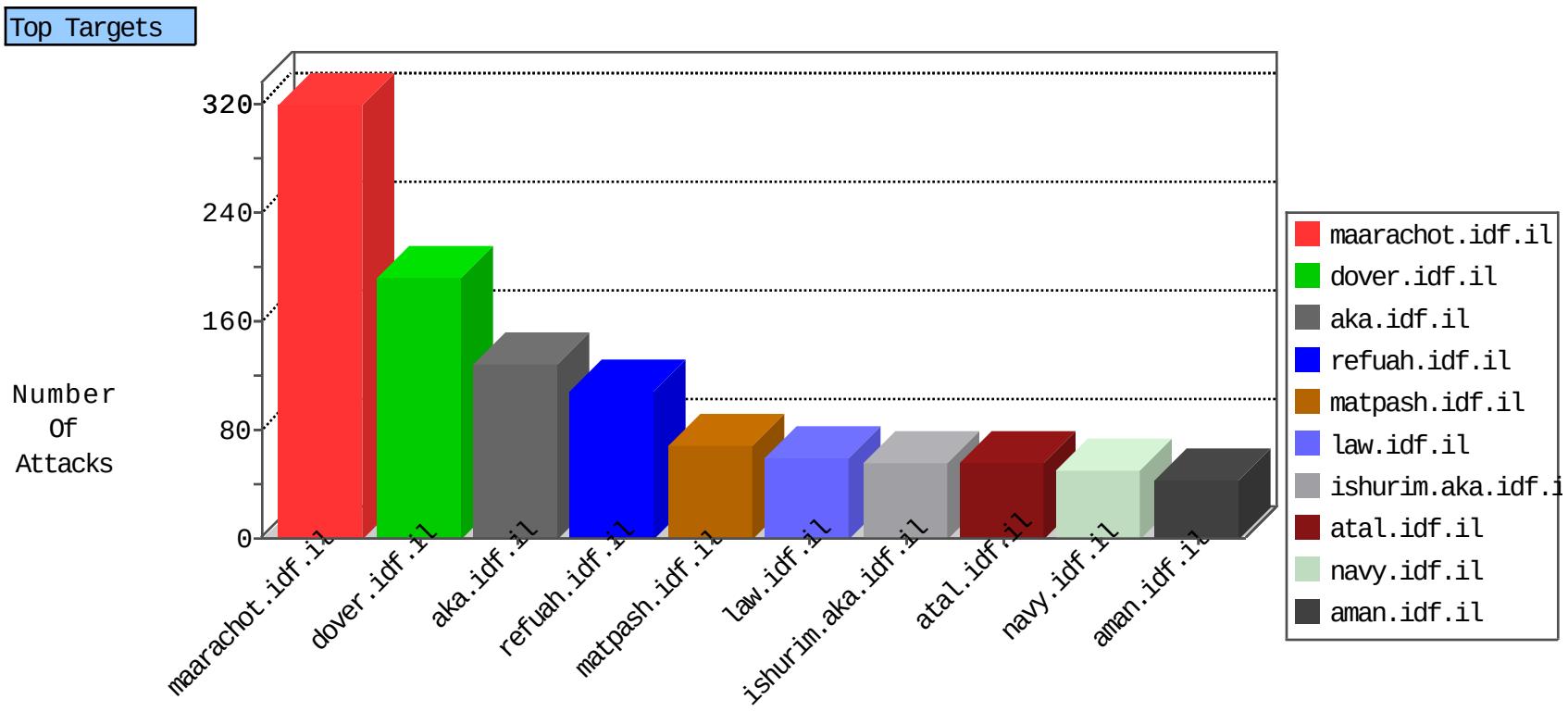
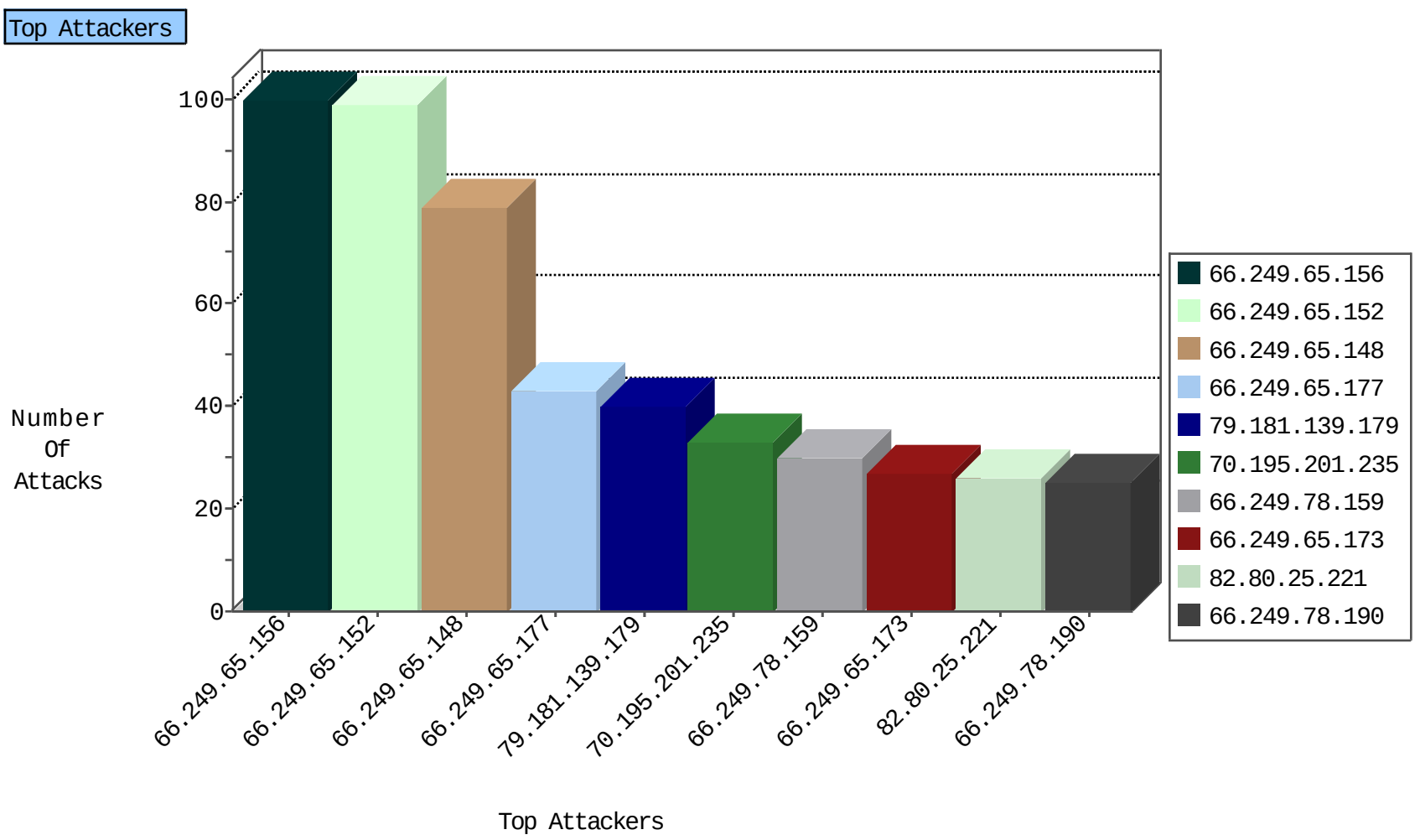
04-05-2015-07:03:04 to 04-05-2015-08:03:04

IDF Under Attack
04-05-2015-07:03:04

Top Targets



Top Attackers



04-05-2015-07:03:04 to 04-05-2015-08:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
79.181.139.179	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	400
80.246.138.156	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	99
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	99
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	79
66.249.65.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	43
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	30
66.249.65.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	27
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	25
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	22
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	21
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	20
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	20
66.249.78.130	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	19
66.249.80.67	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	17
66.249.78.144	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	16
66.249.65.181	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	16
66.249.79.71	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	15
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	15
66.249.79.42	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	14
66.249.78.204	United States	147.237.77.176	matpash.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
66.249.79.26	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	13
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	11
66.249.81.212	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.79.124	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.78.146	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	10
66.249.78.148	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	10
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	9
66.249.73.128	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	8
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.65.187	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	8
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.80.75	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.67.66	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.78.141	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	7
66.249.79.34	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	7
66.249.78.134	United States	147.237.0.34	tikshuv.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	6
66.249.90.86	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	6
66.249.79.55	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	6
66.249.79.140	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.75.31	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	5
66.249.84.188	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.78.137	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.64.118	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
66.249.84.162	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	4

04-05-2015-07:03:04 to 04-05-2015-08:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	22
46.19.85.37	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.255	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.69.98	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.45	e.eitan.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
85.25.43.94	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
213.57.159.49	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.233	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1

04-05-2015-07:03:04 to 04-05-2015-08:03:04

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
37.26.146.158	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
140.119.80.110	Taiwan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
122.228.207.76	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
140.119.80.110	Taiwan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
89.248.162.228	Netherlands	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.61	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
122.228.207.76	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.217	e.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
122.228.207.76	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
140.119.80.110	Taiwan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
104.207.149.204		147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
122.228.207.76	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1

04-05-2015-07:03:04 to 04-05-2015-08:03:04

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
70.195.201.235	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	12
91.200.12.28	Ukraine	147.237.77.176	matpash.idf.il	SAM rule	drop	drop	7
70.195.201.235	United States	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
70.195.201.235	United States	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
70.195.201.235	United States	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
46.19.85.242	Israel	147.237.76.31	nakchal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
46.19.85.255	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
70.195.201.235	United States	147.237.72.166	aka.idf.il	TCP segment out of maximum allowed sequence. Packet dropped.	Streaming Engine: TCP Segment Limit Enforcement	drop	4
46.19.85.255	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
46.19.86.84	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.85.55	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.85.37	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.233	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.187	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
62.219.233.22	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
155.94.254.133		147.237.76.197	e.himush.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
46.19.85.233	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
31.168.79.187	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
176.12.141.91	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
112.111.188.109	China	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
37.26.147.253	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	1
185.2.101.170	Germany	147.237.77.178	e.matpash.idf.il	SAM rule	drop	drop	1
85.15.1.230	Iran, Islamic Republic of	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.99	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.57	United States	147.237.76.148	gqcenter.aka.idf.i		drop	drop	1
38.229.1.15	United States	147.237.76.198	e.yohalan.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
62.219.187.138	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
2.52.43.94	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
149.88.127.27	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.22	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
109.253.151.172	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.210	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
8.37.228.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
46.19.85.37	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
112.25.25.24	China	147.237.76.42	refuah.idf.il	First packet isn't SYN	drop	drop	1

04-05-2015-07:03:04 to 04-05-2015-08:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
62.0.34.177	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	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
188.165.15.198	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2004/january/28.stm	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
37.140.141.27	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	1
192.116.175.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$txtMisparIshi in www.aka.idf.il/main/sachar/	None	1
93.172.44.24	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
184.171.246.30	United States	147.237.76.42	refuah.idf.i	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
46.19.86.199	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.16	Block	1
93.173.151.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
5.29.77.162	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
187.45.241.209	Brazil	147.237.76.42	refuah.idf.i	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
50.31.168.193	United States	147.237.76.42	refuah.idf.i	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
119.81.196.37	Singapore	147.237.76.42	refuah.idf.i	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	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
188.35.138.45	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
31.193.51.80	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1

04-05-2015-07:03:04 to 04-05-2015-08:03:04