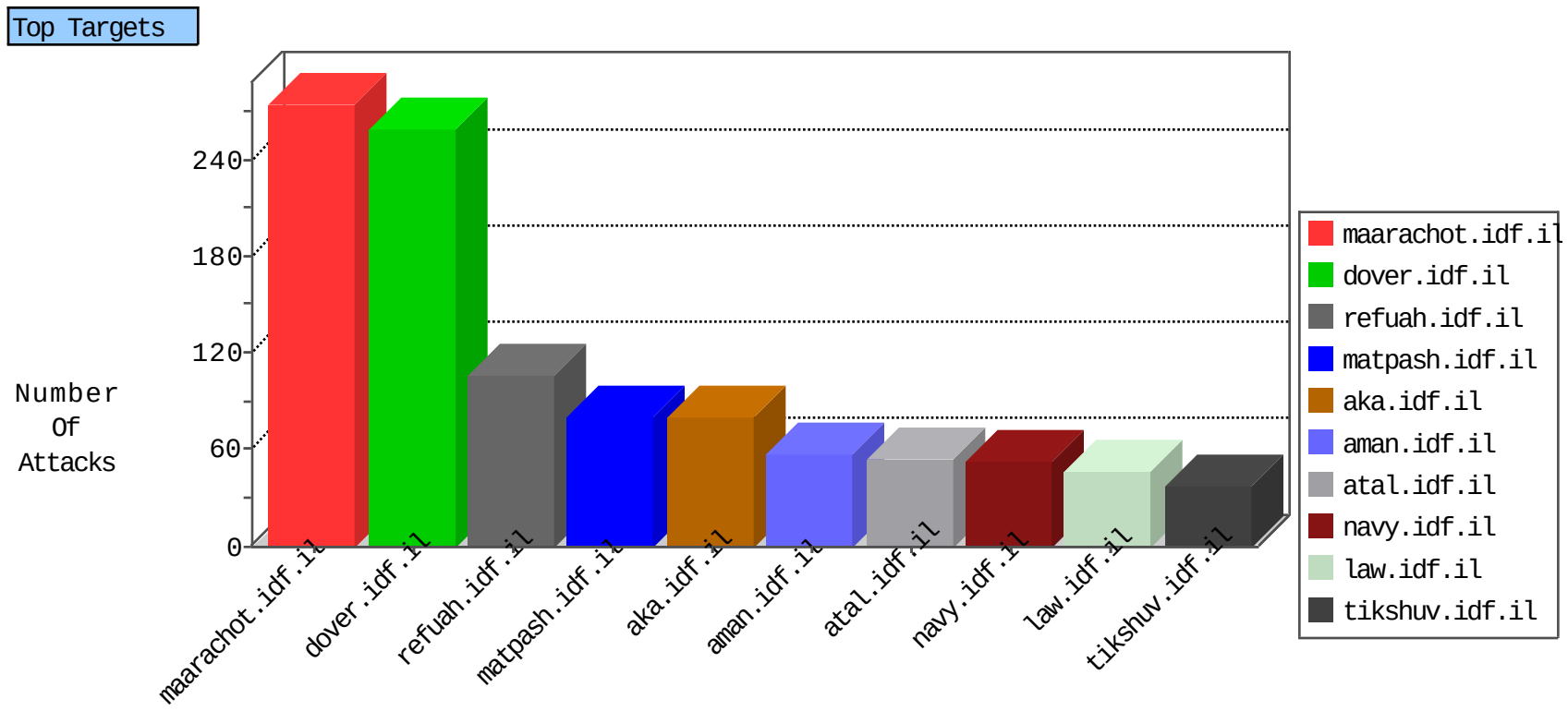
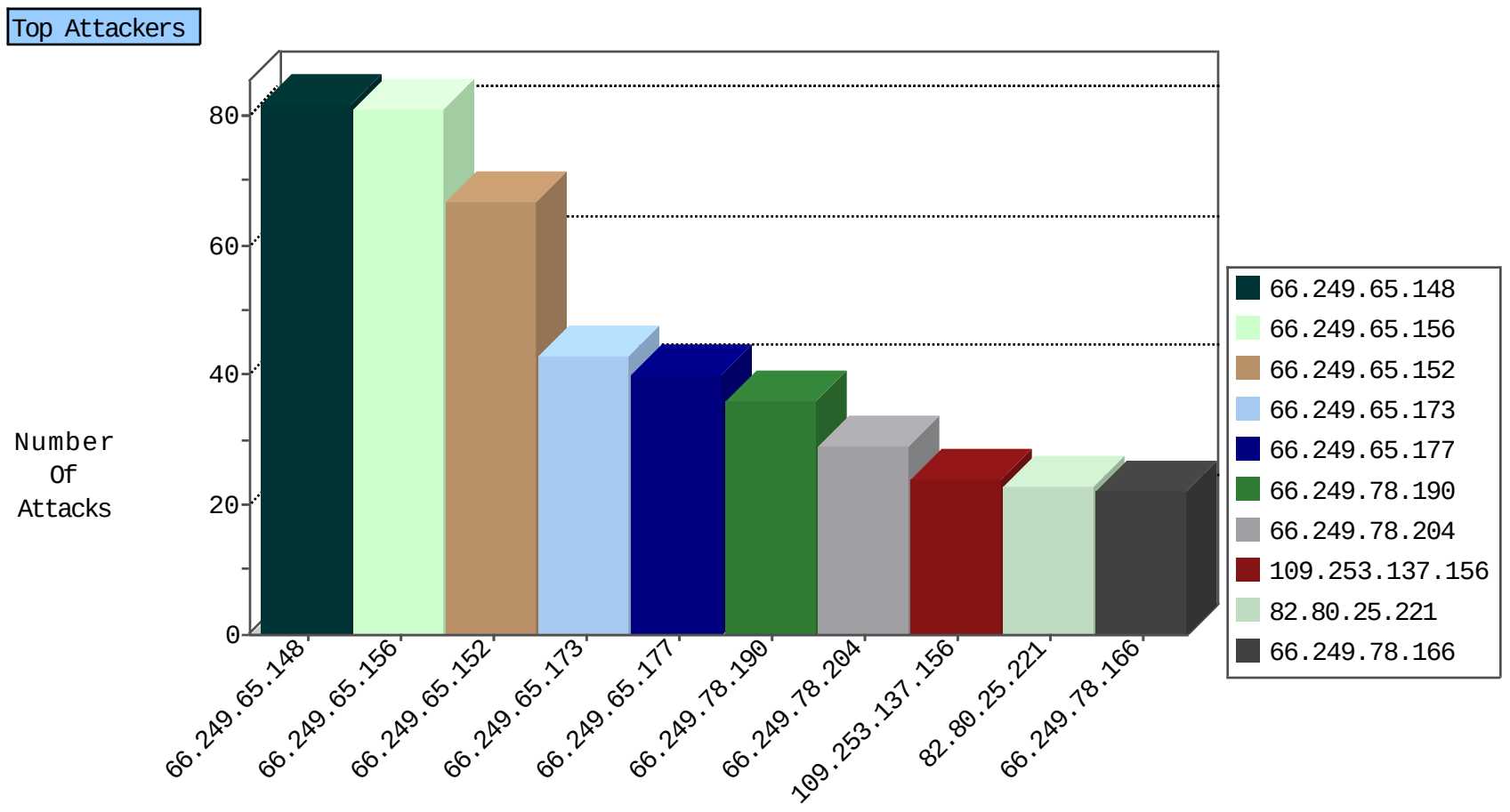
04-05-2015-06:03:00 to 04-05-2015-07:03:00

IDF Under Attack
04-05-2015-06:03:00

Top Targets



Top Attackers



04-05-2015-06:03:00 to 04-05-2015-07:03:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
94.159.207.39	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	82
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	81
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	67
66.249.65.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	43
66.249.65.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	40
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	36
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	29
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	22
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	21
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	20
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	20
66.249.65.181	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	19
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	18
66.249.65.195	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	18
66.249.79.71	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	18
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	15
66.249.79.63	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	15
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.79.124	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	13
66.249.79.26	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	13
66.249.78.137	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	12
66.249.78.130	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
66.249.78.134	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	11
66.249.78.146	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.153	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.144	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
66.249.67.58	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.79.140	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.79.42	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.79.55	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	10
66.249.65.191	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	9
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	9
66.249.65.187	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	9
66.249.79.34	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.78.96	United States	147.237.77.74	law.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
66.249.78.89	United States	147.237.77.74	law.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
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	6
66.249.78.2	United States	147.237.72.166	aka.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
66.249.79.24	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	6
66.249.78.141	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	6
66.249.78.22	United States	147.237.77.74	law.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

04-05-2015-06:03:00 to 04-05-2015-07:03:00

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	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
198.20.69.98	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1

04-05-2015-06:03:00 to 04-05-2015-07:03:00

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
121.240.226.74	India	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	2
61.240.144.64	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.149.161.186	China	147.237.77.19	law-forum.idf.il	GPL SCAN nmap TCP	1
5.255.85.228	Netherlands	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
99.244.135.30	Canada	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
94.182.163.74	Iran, Islamic Republic of	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.85.228	Netherlands	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
99.244.135.30	Canada	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
94.182.163.74	Iran, Islamic Republic of	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1

04-05-2015-06:03:00 to 04-05-2015-07:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
109.253.137.156	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	23
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.253.133.28	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.145.239	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	6
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	5
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	3
208.54.44.203	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
188.138.17.205	France	147.237.76.202	e.halag.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
216.218.206.76	United States	147.237.76.202	e.halag.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
195.88.209.6	Russian Federation	147.237.0.33	idf.il		drop	drop	1
31.168.233.150	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
5.9.97.92	Germany	147.237.76.44	e.refuah.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
208.54.44.203	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
31.168.233.150	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
208.54.44.203	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
188.138.17.205	France	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1

04-05-2015-06:03:00 to 04-05-2015-07:03:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.139.171	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
77.127.176.100	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.132.253	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1674	Block	2
193.93.174.176	Netherlands	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0115-3p2.stm	Block	1
177.190.189.158	Brazil	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0420-2.stm	Block	1
212.227.119.161	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
188.138.17.205	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
37.26.147.228	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
79.178.190.199	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
188.165.15.198	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
37.26.147.228	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1

04-05-2015-06:03:00 to 04-05-2015-07:03:00