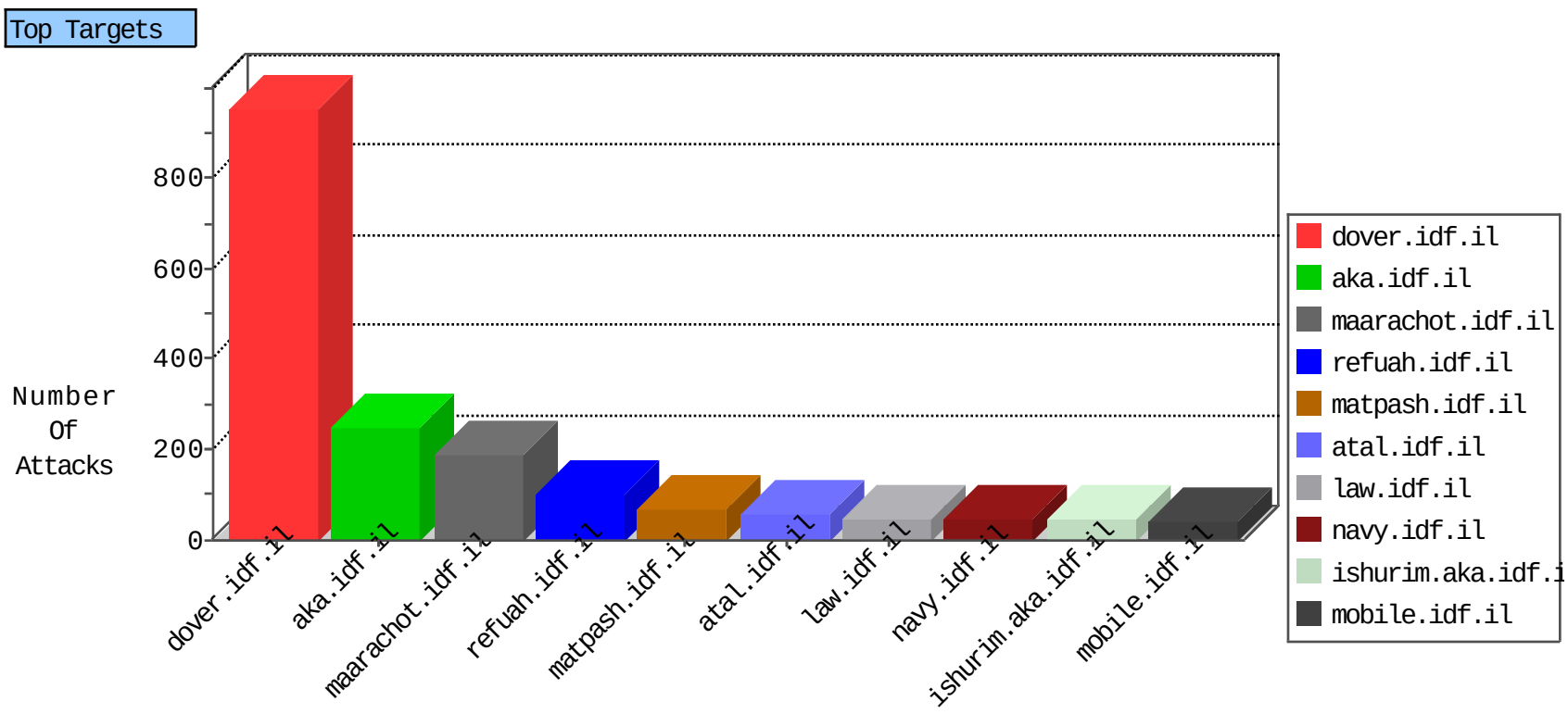
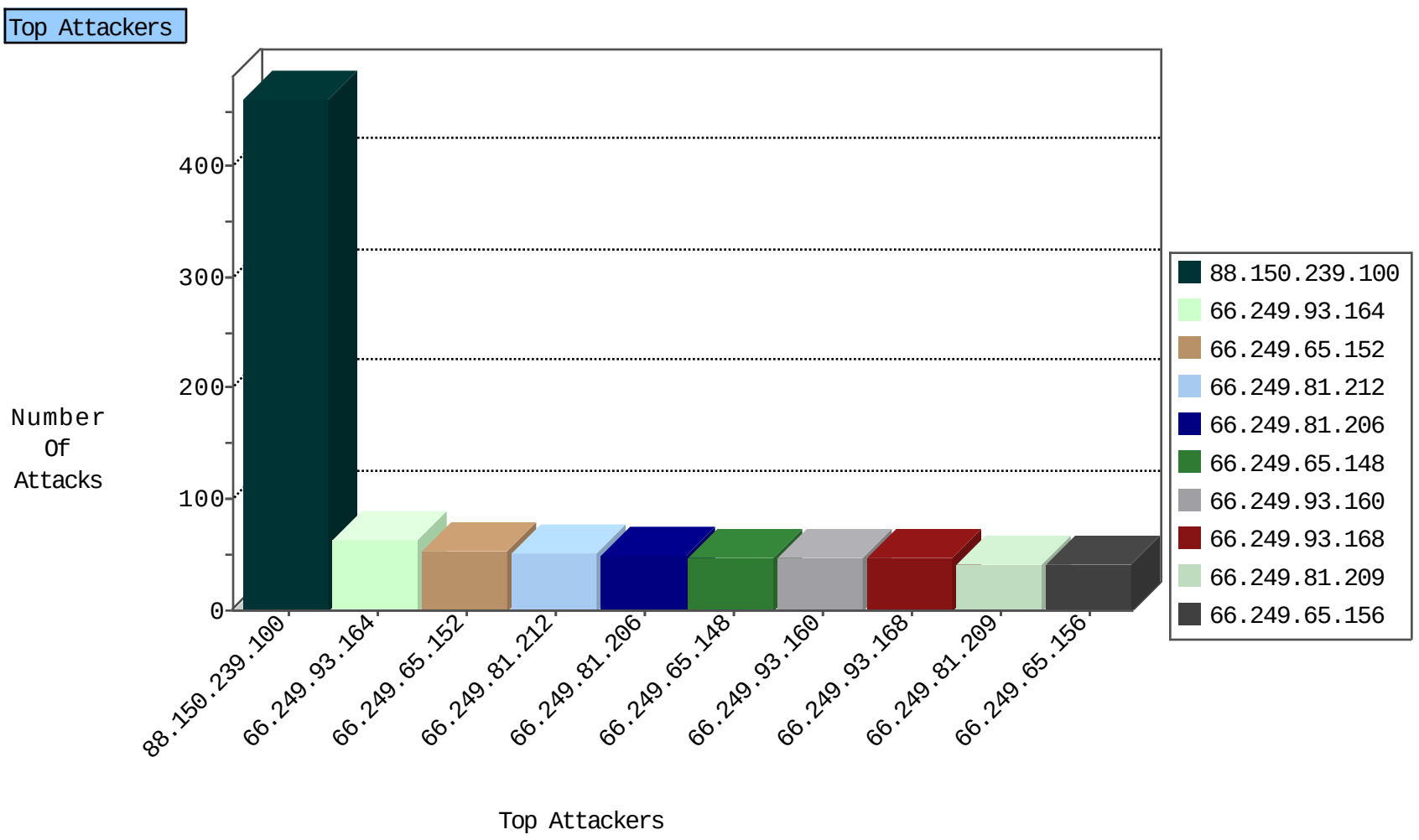
04-05-2015-08:03:07 to 04-05-2015-09:03:07

IDF Under Attack
04-05-2015-08:03:07

Top Targets



Top Attackers



04-05-2015-08:03:07 to 04-05-2015-09:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
88.150.239.100	United Kingdom	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	299
194.90.128.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	245
87.68.33.120	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	63
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	54
66.249.81.206	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	49
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	48
66.249.81.212	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	47
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	47
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	47
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	41
66.249.81.209	United States	147.237.72.166	aka.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	32
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	25
66.249.65.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	23
66.249.78.82	United States	147.237.77.74	law.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
88.150.239.100	United Kingdom	147.237.77.216	dover.idf.il	IIS-Unicode-Dir-Trav-9	dest-reset	16
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	16
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.78.146	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.65.195	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	15
66.249.79.26	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	15
66.249.78.137	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	14
66.249.79.42	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	13
66.249.79.55	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	13
66.249.78.153	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	11
66.249.78.148	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	11
66.249.78.130	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	11
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	11
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.65.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.81.215	United States	147.237.77.216	dover.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
66.249.79.124	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	9
66.249.78.254	United States	147.237.72.166	aka.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
66.249.81.218	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
88.150.239.100	United Kingdom	147.237.77.216	dover.idf.il	Web-etc/passwd-Dir-Traversal	dest-reset	8
66.249.69.99	United States	147.237.76.31	nakchal.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	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	6
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.90.82	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	5
79.181.139.179	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	5
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5

04-05-2015-08:03:07 to 04-05-2015-09:03:07

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	29
192.116.177.146	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
37.247.97.194	Turkey	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	2
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
5.28.183.190	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.25.43.94	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.64	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1

04-05-2015-08:03:07 to 04-05-2015-09:03:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
2.52.175.156	Israel	147.237.77.243	mobile.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	30
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
221.235.188.212	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
208.39.68.33	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
188.138.9.51	Germany	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
91.238.134.92	Poland	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
37.247.97.194	Turkey	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
5.255.85.228	Netherlands	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
208.39.68.33	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
178.19.107.114	Poland	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
132.74.95.19	Israel	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
221.235.188.212	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
5.255.85.228	Netherlands	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
221.235.188.212	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1

04-05-2015-08:03:07 to 04-05-2015-09:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
88.150.239.100	United Kingdom	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	158
24.215.190.116	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	26
109.253.142.131	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.143.133	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
82.80.42.188	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
168.63.139.43	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
80.246.130.188	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	13
109.253.138.163	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
82.80.42.176	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
62.210.141.227	France	147.237.76.42	refuah.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	8
46.19.86.44	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
134.191.232.68	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.143.145	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.157.94	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
2.52.175.156	Israel	147.237.77.243	mobile.idf.il	First packet isn't SYN	drop	drop	5
46.19.86.92	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
2.52.175.156	Israel	147.237.77.243	mobile.idf.il	TCP segment with urgent pointer (no data). Urgent data indication was stripped. Please refer to sk36869.	Streaming Engine: TCP Urgent Data Enforcement	drop	5
70.39.186.218	Satellite Provider	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	5
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	4
88.150.239.100	United Kingdom	147.237.77.216	dover.idf.il	'Cookie' header length exceeded maximum allowed length	HTTP Format Sizes	monitor	4
46.19.85.105	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	3
46.19.86.110	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.85.64	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.85.108	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
84.108.43.246	Israel	147.237.77.234	halag.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
98.143.148.107	United States	147.237.76.148	gqcenter.aka.idf.i		drop	drop	2
109.253.128.49	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
212.117.136.6	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
109.253.141.255	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
212.199.251.227	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.57	United States	147.237.76.44	e.refuah.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
70.39.187.112	Satellite Provider	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	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
141.212.122.53	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
212.199.251.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
8.37.228.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
188.138.17.205	France	147.237.77.61	e.cogat.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.142	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.54	United States	147.237.0.33	idf.il		drop	drop	1
84.111.155.127	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
176.67.126.125	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
212.117.136.6	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.19.85.145	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.54	United States	147.237.77.121	e.navy.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
5.9.97.92	Germany	147.237.76.197	e.himush.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
84.111.155.127	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

04-05-2015-08:03:07 to 04-05-2015-09:03:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.50.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	11
88.150.239.100	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 88.150.239.100	Block	5
46.19.85.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	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
195.244.23.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter moduleT.oGoTo in www.aka.idf.il/main/giyus/login.aspx	None	1
62.90.35.105	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
2.52.181.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
174.130.219.16	United States	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
84.228.195.186	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
46.19.86.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/theproj/	Block	1
109.253.159.185	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
62.210.141.227	France	147.237.76.42	refuah.idf.il	Admin Blocking	Block	1
174.130.219.16	United States	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/soldiercontact.aspx	None	1
87.68.80.126	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.114.21	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __EVENTVALIDATION in aka.idf.il/main/sachar/	None	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/faq.aspx	Block	1
125.209.235.178	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
67.1.253.111	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/homefront3.stm	Block	1
2.54.183.136	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
194.90.128.25	Israel	147.237.72.167	ishurim.aka.idf.i	Multiple Untraceable SSL Sessions from 194.90.128.25 (Unknown SSL Session)	None	1
87.69.4.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
46.120.114.21	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/payslips.aspx	None	1
212.179.162.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
46.19.85.22	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
194.90.128.25	Israel	147.237.72.167	ishurim.aka.idf.i	SSL Untraceable Connection - Unknown SSL Session	None	1
88.150.239.100	United Kingdom	147.237.77.216	dover.idf.il	Multiple Acunetix scanner attack(+) from 88.150.239.100	Block	1
46.121.247.55	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
80.246.130.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/templates/sendtofriend/sendtofriend.aspx	Block	1

04-05-2015-08:03:07 to 04-05-2015-09:03:07