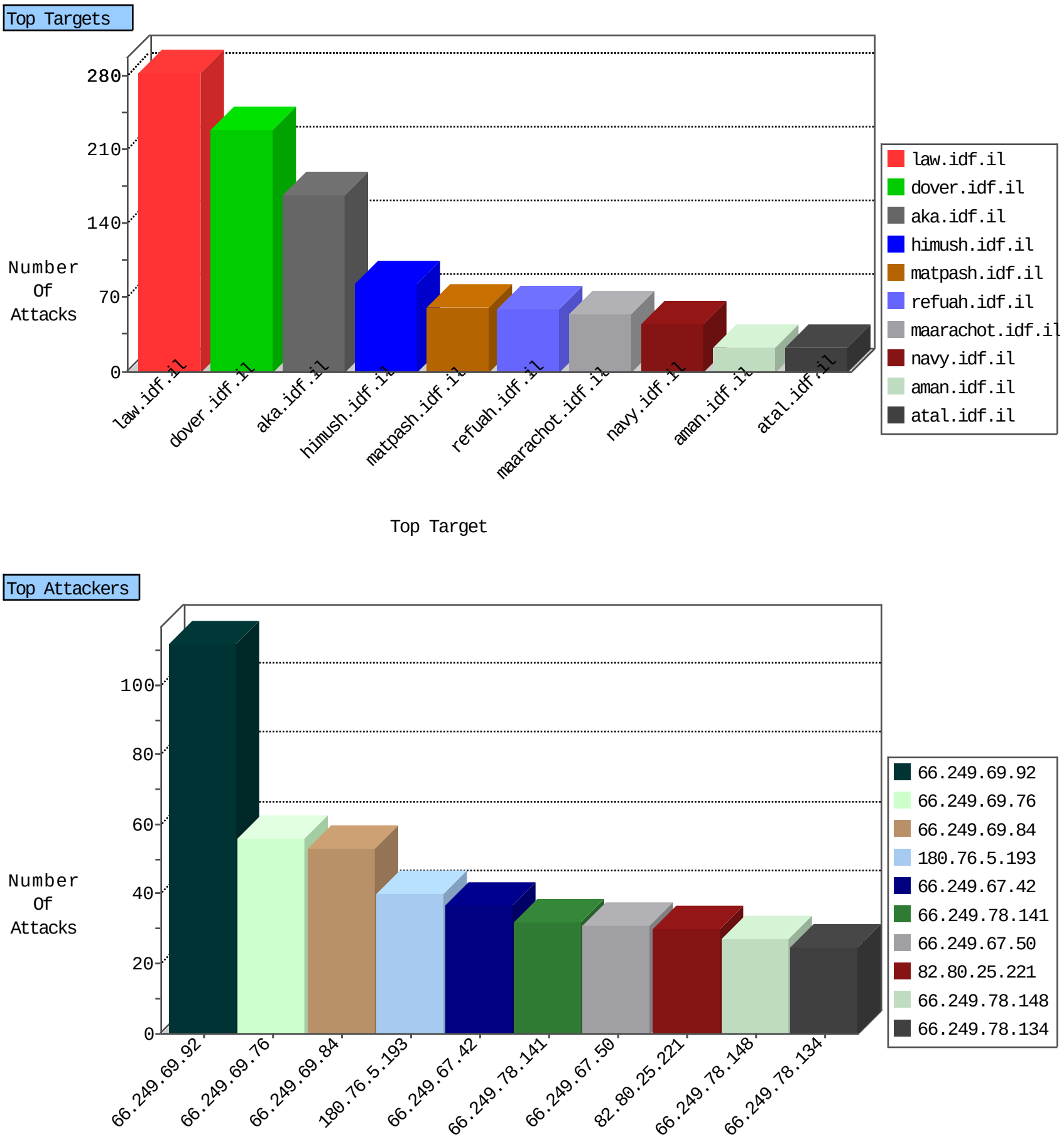
04-03-2015-19:03:04 to 04-03-2015-20:03:04

IDF Under Attack
04-03-2015-19:03:04



04-03-2015-19:03:04 to 04-03-2015-20:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.69.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	110
46.117.160.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
66.249.69.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	56
66.249.69.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	53
66.249.78.141	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	32
66.249.67.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	31
66.249.67.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	28
66.249.78.148	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	27
66.249.78.28	United States	147.237.76.42	refuah.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	24
66.249.78.134	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	23
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	19
66.249.64.110	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	18
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	16
66.249.67.5	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.67.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.81.179	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	14
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	13
66.249.75.60	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.81.175	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.67.13	United States	147.237.72.166	aka.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
66.249.84.188	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.67.157	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.64.118	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	9
66.249.67.42	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	9
66.249.67.31	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	8
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	8
66.249.92.22	United States	147.237.77.170	maarachot.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
66.249.81.183	United States	147.237.77.74	law.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
66.249.67.34	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	7
66.249.75.68	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.78.201	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	6
66.249.78.61	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	6
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.83.153	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.78.37	United States	147.237.77.234	halag.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	6
66.249.78.184	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	5
66.249.75.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.67.41	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	5
66.249.92.29	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	5
66.249.75.95	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	5
66.249.78.47	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	5

04-03-2015-19:03:04 to 04-03-2015-20:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	40
79.178.132.153	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
46.116.222.190	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
72.197.194.122	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1

04-03-2015-19:03:04 to 04-03-2015-20:03:04

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
122.228.207.77	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
99.244.135.30	Canada	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.67	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.166.189.69	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
61.166.189.69	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.41.39.125	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
183.136.216.7	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243		147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
61.166.189.69	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
59.41.39.125	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
2.54.170.219	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.77	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1

04-03-2015-19:03:04 to 04-03-2015-20:03:04

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	30
109.253.145.223	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.158.150	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
109.253.145.46	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
79.178.132.153	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	6
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
109.253.146.236	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
2.54.170.219	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
2.54.170.219	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
2.54.170.219	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
46.19.85.93	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
64.246.165.200	United States	147.237.77.233	atal.idf.il	header rejection pattern found in request	Header Rejection	monitor	3
188.120.148.158	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
5.22.130.150	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	3
46.19.85.98	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
176.12.141.31	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
207.241.237.211	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
37.46.39.40	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
176.12.151.26	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
85.64.39.192	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
141.212.122.174	United States	147.237.77.227	e.hamaz.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
109.253.135.240	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
37.124.47.186	Saudi Arabia	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
2.54.143.153	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
85.64.39.192	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.175	United States	147.237.76.44	e.refuah.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
109.253.135.240	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
79.178.1.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
37.124.47.186	Saudi Arabia	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
188.138.1.218	Germany	147.237.72.217	e.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
2.54.143.153	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.68	United States	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
85.64.214.7	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
5.22.130.150	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
141.212.122.177	United States	147.237.76.198	e.yohalan.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.53	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
198.20.69.74	United States	147.237.76.34	yohalan.idf.il		drop	drop	1
2.54.143.153	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
141.212.122.70	United States	147.237.8.14	e.orchot.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
85.64.214.7	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.93	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
141.212.122.172	United States	147.237.77.121	e.navy.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
95.253.2.26	Italy	147.237.72.166	aka.idf.il	illegal header format detected: Malformed HTTP protocol name in response	Block HTTP Non Compliant	monitor	1
46.19.85.172	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

04-03-2015-19:03:04 to 04-03-2015-20:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
95.253.2.26	Italy	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	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
67.186.32.148	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	2
109.253.156.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
79.178.132.153	Israel	147.237.76.42	refuah.idf.i	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
95.223.126.222	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.156.206	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.183.33.247	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
37.142.223.136	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
79.160.83.68	Norway	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
176.12.141.22	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.230.100.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.186.151.102	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
79.176.2.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/default.aspx	None	1
203.133.169.12	Korea, Republic of	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.108.248.125	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.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
109.226.35.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.178.25.167	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
203.133.169.157	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/press_conference_16may00.stm	Block	1
93.172.172.94	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/april/03b.stm	Block	1

04-03-2015-19:03:04 to 04-03-2015-20:03:04