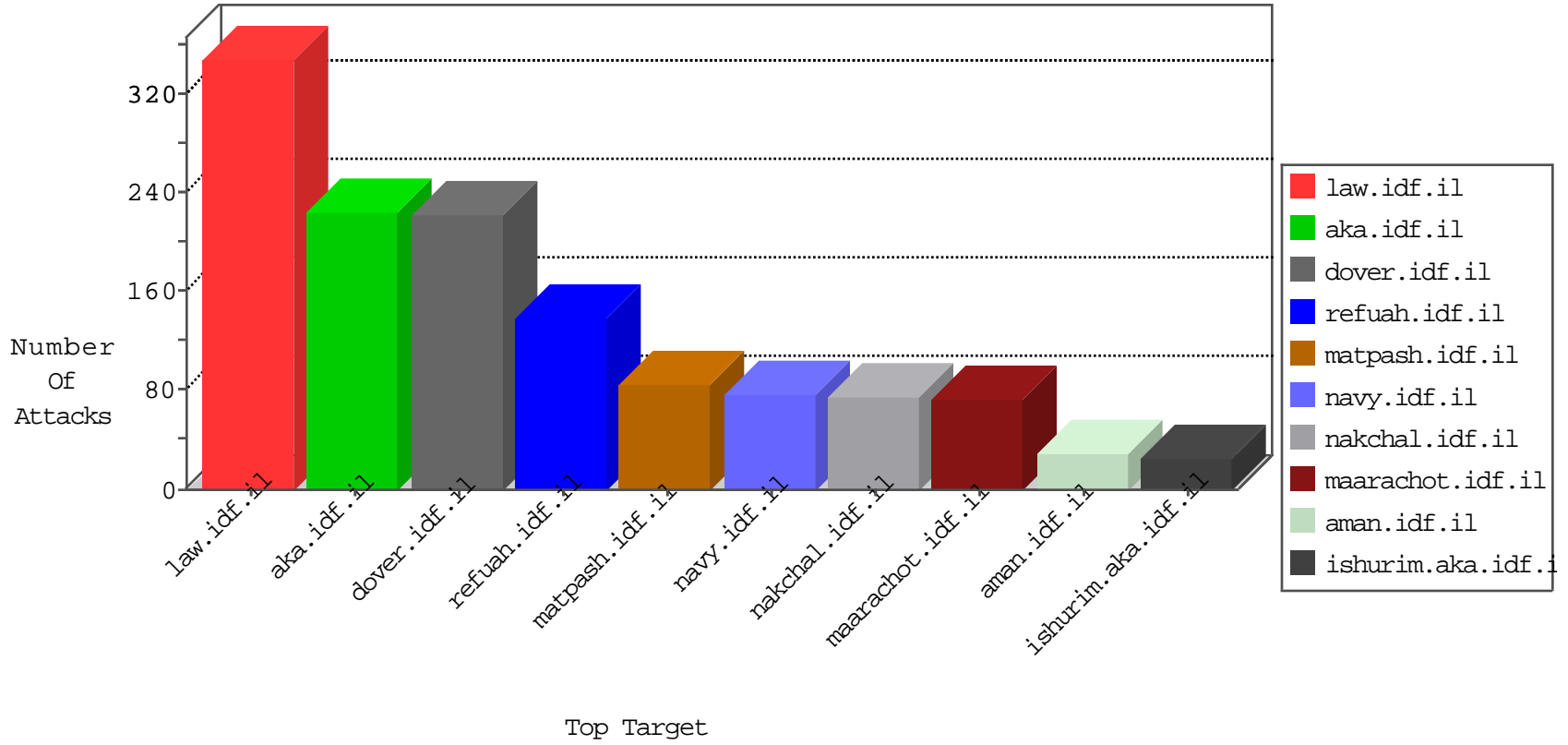
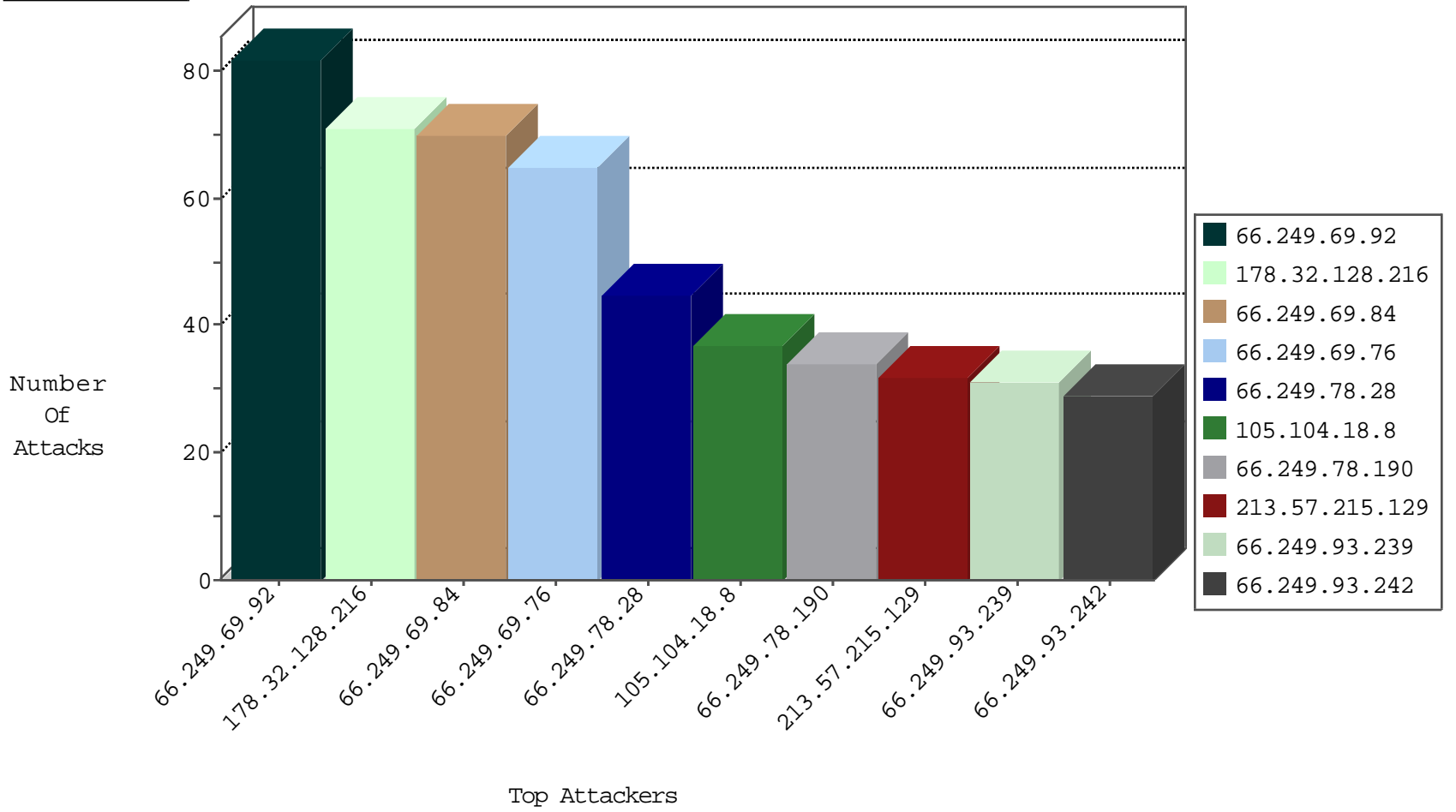




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
79.178.177.132	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	216
66.249.69.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	82
66.249.69.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	66
66.249.69.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	65
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	45
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	34
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	31
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	29
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	28
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	26
66.249.78.14	United States	147.237.76.42	refuah.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	25
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	25
66.249.93.234	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	24
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	20
105.104.2.204	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	19
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.75.60	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	18
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.67.157	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	18
66.249.67.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	17
66.249.67.13	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	16
66.249.75.68	United States	147.237.77.74	law.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	16
66.249.78.184	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	15
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	14
66.249.93.237	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	14
66.249.64.118	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	13
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	13
66.249.64.114	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	13
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
66.249.67.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.75.95	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	11
66.249.64.110	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	11
105.104.18.8	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	11
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	10
66.249.67.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.75.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.93.131	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.78.38	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	8
66.249.78.44	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	8
66.249.78.187	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	8
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.67.124	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	7
66.249.64.123	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.78.51	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	6
66.249.93.254	United States	147.237.77.74	law.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	5
66.249.78.120	United States	147.237.0.34	tikshuv.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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
198.20.70.114	United States	147.237.77.170	maarachot.idf.il	DVRep_P-N_40-59	Permit	22
5.29.53.20	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.117.62.67	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.180.54.144	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.186.133.232	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
83.226.154.245	Sweden	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.120.27.62	Romania	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
80.246.137.42	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.0.33	idf.il	DVRep_P-N_40-59	Permit	1
85.25.43.94	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.250.218.222	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
105.104.18.8	Algeria	147.237.77.216	dover.idf.il	ET CURRENT_EVENTS High Orbit Ion Cannon (HOIC) Attack Inbound Generic Detection Double Spaced UA	9
105.104.2.204	Algeria	147.237.77.216	dover.idf.il	ET CURRENT_EVENTS High Orbit Ion Cannon (HOIC) Attack Inbound Generic Detection Double Spaced UA	9
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
5.29.207.9	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.130		147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
177.129.79.177	Brazil	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
58.20.54.249	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
177.129.79.177	Brazil	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
8.29.144.205	United States	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
89.248.162.228	Netherlands	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
177.129.79.177	Brazil	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
8.29.144.205	United States	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 2048	1
122.228.207.77	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
8.29.144.205	United States	147.237.72.156	aman.idf.il	ET SCAN NMAP -f -sS	1
122.228.207.77	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
178.32.128.216	France	147.237.77.74	law.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	70
213.57.215.129	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	32
105.104.18.8	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
176.12.141.149	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
41.196.79.106	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
37.142.98.69	Israel	147.237.0.19	madim.atal.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
85.64.243.220	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
85.64.243.220	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
5.29.153.115	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
91.200.12.55	Ukraine	147.237.77.176	matpash.idf.il	SAM rule	drop	drop	3
41.218.168.44	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
103.231.161.86		147.237.77.216	dover.idf.il	SAM rule	drop	drop	2
79.179.166.18	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.62	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
5.102.254.179	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.159	United States	147.237.76.200	eitan.aka.idf.il		drop	drop	1
50.74.50.202	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
37.142.207.134	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
198.20.69.74	United States	147.237.8.45	e.eitan.idf.il	SAM rule	drop	drop	1
141.212.122.82	United States	147.237.76.198	e.yohalan.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
84.109.0.86	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.98	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
37.46.39.122	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
74.82.47.39	United States	147.237.76.198	e.yohalan.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
41.196.79.106	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
213.57.45.159	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.84	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.106	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
77.125.18.79	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
5.22.130.194	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.91	United States	147.237.76.196	e.sviva.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.106	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
37.142.100.10	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
184.105.139.76	United States	147.237.0.33	idf.il		drop	drop	1
112.111.188.109	China	147.237.77.216	dover.idf.il	SAM rule	drop	drop	1
79.178.122.41	Israel	147.237.72.166	aka.idf.il	Invalid checksum. Packet dropped.	Streaming Engine: TCP Invalid Checksum	drop	1
141.212.122.92	United States	147.237.77.61	e.cogat.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
85.65.228.88	Israel	147.237.76.31	nakchal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.160	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
37.142.207.134	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
188.120.148.235	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.121.128	United States	147.237.8.14	e.orchot.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1

04-04-2015-13:03:08 to 04-04-2015-14:03:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.98	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	16
85.64.66.173	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
188.165.15.198	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.198	Block	4
77.125.156.137	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	4
109.186.133.232	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	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
176.12.140.149	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	2
109.65.51.129	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
198.20.70.114	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
46.117.62.67	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/webresource.axd	Block	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/0307-1.stm	Block	1
79.181.55.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
2.54.30.169	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
46.120.95.180	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/authenticationservice.aspx/getuserdetails	Block	1
208.113.224.193	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-admin/	Block	1
83.222.232.214	United Kingdom	147.237.72.156	aman.idf.il	Unauthorized Method HEAD for /	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0302-3.stm	Block	1
178.32.128.216	France	147.237.77.74	law.idf.il	Web leech 6	Block	1
69.164.231.219	United States	147.237.77.19	law-fonum.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
212.116.166.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
31.168.210.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1

04-04-2015-13:03:08 to 04-04-2015-14:03:08