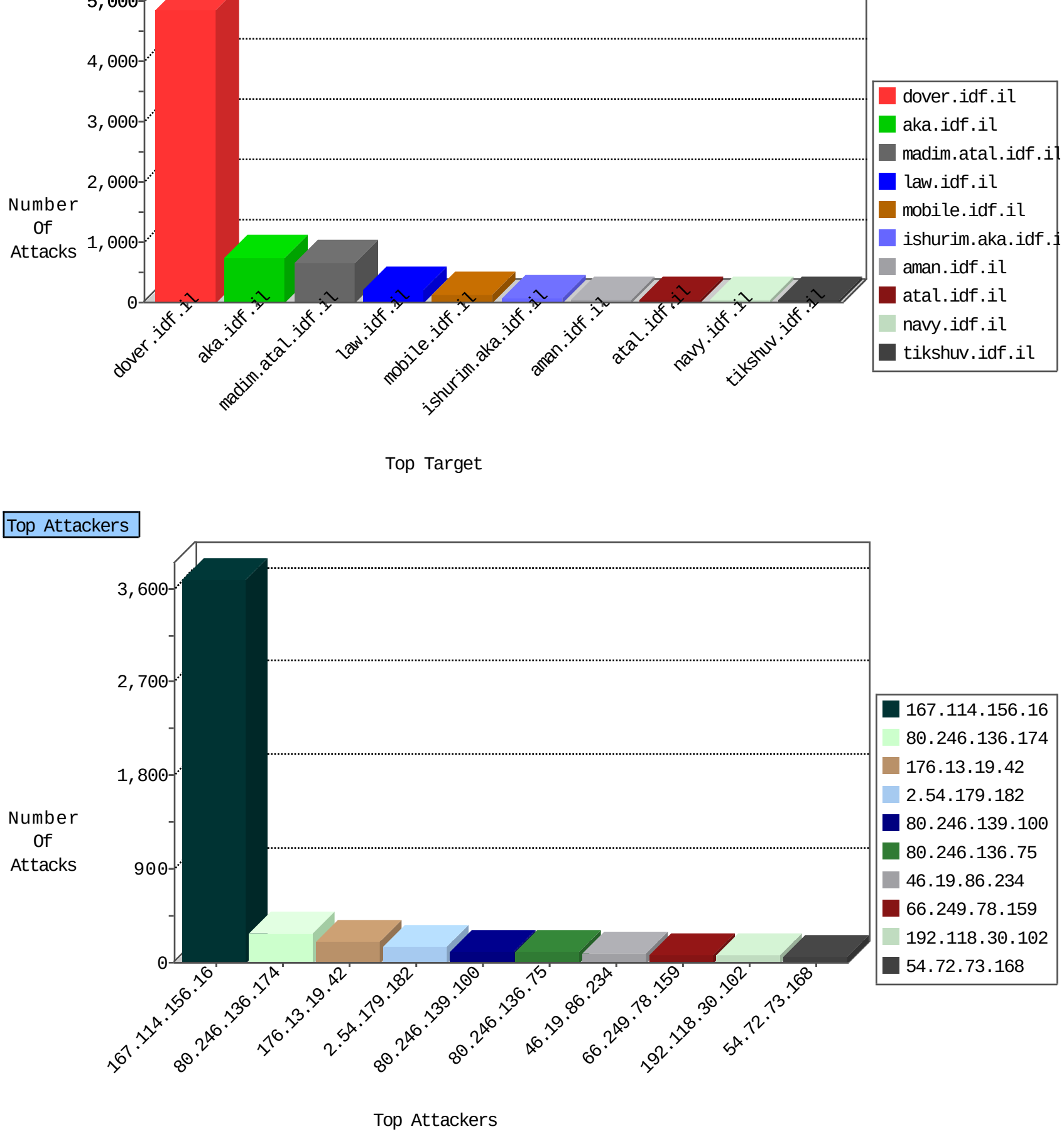
12-28-2015-15:04:04 to 12-28-2015-16:04:04

IDF Under Attack Daily Report



12-28-2015-15:04:04 to 12-28-2015-16:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3116
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2817
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	481
82.178.149.166	Oman	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	120
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
66.249.78.159	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	58
66.249.93.99	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	45
66.249.78.166	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	36
66.249.93.103	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	34
37.26.148.254	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	32
58.187.75.183	Vietnam	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	21
193.190.220.200	Belgium	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
198.103.104.11	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
66.249.92.32	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
66.249.92.26	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
107.178.194.87	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
66.249.66.28	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
66.249.93.107	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
65.19.138.34	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
54.240.197.226	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
54.240.197.226	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
46.236.24.51	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
37.8.111.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
65.19.138.34	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
69.40.44.245	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
204.13.200.200	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
66.249.93.107	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
107.170.142.158	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
208.184.112.74	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
104.131.226.73	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
45.35.64.142		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
69.40.44.245	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
37.26.148.254	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
37.26.148.179	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
66.249.93.103	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
212.179.64.162	Israel	147.237.72.167	ishurim.aka.idf.i	Block_Udp_All_Nets	drop	3
69.175.127.10	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
66.220.146.28	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
65.19.138.33	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
115.134.209.128	Malaysia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
58.187.75.183	Vietnam	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	3

12-28-2015-15:04:04 to 12-28-2015-16:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-28-2015-15:04:04 to 12-28-2015-16:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.86.51	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	11
109.253.215.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.236.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.85.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.47.229.34	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
5.102.203.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.63	147.237.8.45		e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
131.109.15.15	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
109.66.56.133	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.189.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
168.62.238.153	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.63	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.72.156		aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

12-28-2015-15:04:04 to 12-28-2015-16:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1819
176.13.19.42	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	108
176.13.19.42	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	87
31.171.244.115	Switzerland	147.237.77.216	dover.idf.il	drop	SAM rule	drop	61
196.217.188.171	Morocco	147.237.77.216	dover.idf.il	drop		drop	57
2.54.179.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	53
213.8.204.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
2.54.179.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
2.54.179.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	22
82.81.5.83	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
176.13.20.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
2.54.179.182	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	20
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.19.85.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
80.246.136.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.148.254	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
2.54.179.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
79.182.194.2	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
66.249.79.84	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
81.218.22.216	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.54.179.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
79.177.169.3	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
81.218.22.216	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.52.33.119	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.51	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
79.178.58.248	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.75	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.168.238.114	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
79.181.230.176	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.78.159	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
198.103.104.11	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
66.249.78.159	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
217.132.15.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.3.146.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.37.129	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
31.154.135.2	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
109.66.56.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

12-28-2015-15:04:04 to 12-28-2015-16:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	159
80.246.136.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.86.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
80.246.139.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
80.246.136.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
80.246.139.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	26
80.246.136.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
93.173.170.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
46.121.199.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.85.171	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.13.20.88	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	5
109.253.129.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
80.246.137.212	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Email in mobile.idf.il/sachar/createaccount	Block	4
212.199.101.60	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
80.246.137.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.4.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.1.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	3
46.19.85.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.140.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
176.13.3.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.90.143.230	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.183.183.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/mas.aspx	Block	2
176.12.136.241	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
46.19.86.197	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.250.113.144	Israel	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
80.246.137.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.126	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.126.34.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
46.117.109.235	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
80.246.136.174	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
66.220.159.119	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.214.89	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
37.26.148.149	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/mobile/templates/catalog/catalog.aspx	Block	1
2.54.156.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.194.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.88.153.140	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.86.75	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.140.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1
188.121.37.183	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
77.125.117.74	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
46.19.85.34	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.16.33	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1

12-28-2015-15:04:04 to 12-28-2015-16:04:04