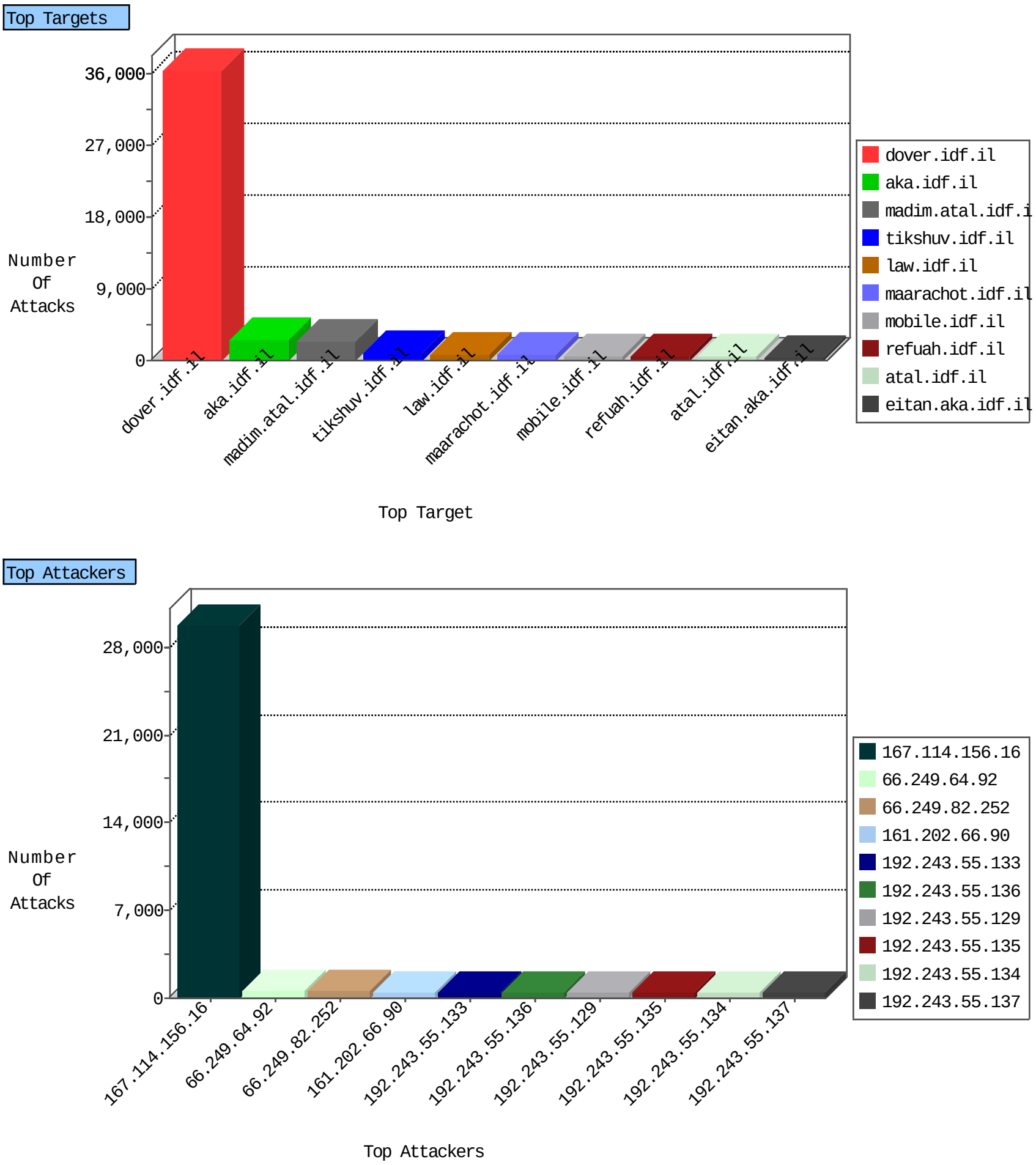
03-12-2016 to 03-13-2016

IDF Under Attack
Daily Report



03-12-2016 to 03-13-2016

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	91171
161.202.66.90	Netherlands	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	1782
46.19.86.108	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	263
37.26.148.150	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	forward	206
82.145.222.111	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	130
82.145.220.162	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	117
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	73
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	45
82.145.218.138	Europe	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	26
175.139.170.130	Malaysia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	23
82.145.211.6	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	20
82.145.211.100	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
82.145.220.82	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
82.145.210.188	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
82.145.216.177	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
82.145.220.147	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
82.145.217.85	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
82.145.223.136	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
82.145.221.54	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
41.238.31.171	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
82.145.209.29	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	4
134.147.203.115	Germany	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	4
200.160.6.137	Brazil	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	4
79.182.38.184	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
8.37.231.89	Anonymous Proxy	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
134.147.203.115	Germany	147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	3
82.145.221.241	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3
79.182.38.184	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	2
80.82.64.220	Netherlands	147.237.72.156	aman.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
146.185.239.100	Russian Federation	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
134.147.203.115	Germany	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	2
162.248.100.195	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2
74.217.28.153	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
134.147.203.115	Germany	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	2
125.27.5.150	Thailand	147.237.72.166	aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
146.185.239.100	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	2
134.147.203.115	Germany	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	2
125.65.46.143	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
134.147.203.115	Germany	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	2
8.37.231.89	Anonymous Proxy	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
146.185.239.100	Russian Federation	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
126.46.7.121	Japan	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	2
104.196.19.51	United States	147.237.8.46	e.chinuch.idf.il	Invalid TCP Flags	drop	2
134.147.203.115	Germany	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	2
66.240.192.138	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.84	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1

03-12-2016 to 03-13-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	22
106.120.173.118	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	20
5.29.187.252	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
109.65.50.71	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	17
37.142.68.86	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	12
79.183.192.9	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
79.180.112.141	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
89.138.83.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
109.64.188.218	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
77.125.77.127	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
31.154.168.132	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.181.0.128	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
89.139.244.147	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	8
93.63.188.181	Italy	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
87.69.127.55	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
107.150.56.254	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	7
79.178.132.91	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
93.172.157.122	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
79.182.38.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
109.160.151.84	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
5.102.206.148	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.65.11.200	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
159.122.222.194	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	20086: HTTP: Mueblackcat Security Scanner	Block	4
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
177.185.192.50	Brazil	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
203.171.33.38	New Zealand	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
5.9.85.4	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
82.166.247.138	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.65.25.198	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
5.22.135.219	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
159.122.222.194	Netherlands	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Mueblackcat Security Scanner	Block	4
94.102.153.58	United Kingdom	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
62.210.225.135	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
87.242.112.35	Russian Federation	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
184.173.233.226	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
209.15.196.171	Canada	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
95.86.79.172	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
213.8.145.99	Israel	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
144.76.93.46	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
80.246.133.205	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
66.249.93.121	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
176.228.68.96	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
78.46.196.116	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
65.55.210.32	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
83.149.126.98	Netherlands	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
46.19.85.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
5.9.85.4	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2

03-12-2016 to 03-13-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.92	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	581
66.249.82.252	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	533
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	95
94.102.153.58	147.237.77.176	United Kingdom	matpash.idf.il	SQL Injection - Select From	12
213.8.145.99	147.237.76.42	Israel	refuah.idf.il	SQL Injection - Select From	12
62.210.225.135	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	12
93.63.188.181	147.237.77.226	Italy	www.chamatz.aka.idf.il	SQL Injection - Select From	8
87.242.112.35	147.237.76.42	Russian Federation	refuah.idf.il	SQL Injection - Select From	6
177.185.192.50	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	6
209.15.196.171	147.237.76.86	Canada	navy.idf.il	SQL Injection - Select From	6
80.246.133.115	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	6
184.173.233.226	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
176.13.7.106	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
2.54.161.192	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
66.249.65.224	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	4
203.171.33.38	147.237.76.86	New Zealand	navy.idf.il	SQL Injection - Select From	4
176.13.15.192	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
109.253.215.2	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
161.202.66.90	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	3
109.253.223.109	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
61.153.237.122	147.237.0.19	China	madim.atal.idf.il	GPL SCAN nmap TCP	2
66.249.93.95	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
109.64.149.100	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.66.39	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.9	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
197.52.224.68	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP adminlogin access	2
197.52.198.220	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP login.htm access	2
94.102.48.194	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
5.29.187.252	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.93.91	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.125	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.25	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.68	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sA (2)	2
45.79.81.142	147.237.72.156		aman.idf.il	ET WEB_SERVER Poison Null Byte	1
185.72.179.221	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.118	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.194	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.49.74	147.237.76.201	France	e.atal.idf.il	ET SCAN Potential SSH Scan	1
13.68.31.54	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
104.197.254.53	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
82.117.208.243	147.237.0.15		kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
202.71.25.29	147.237.77.235	India	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
93.113.125.12	147.237.8.14	Romania	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
208.71.68.132	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
58.253.96.122	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 2048	1

03-12-2016 to 03-13-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.228.186.4	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	280
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	186
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	167
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	118
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	116
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	108
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	107
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	94
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	93
79.178.174.211	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	93
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	91
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	87
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	87
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	83
37.238.162.38	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	78
37.238.162.38	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	78
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	78
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	77
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	75
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	75
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	73
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	73
8.37.231.89	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	69
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	68
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	67
176.13.13.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
80.246.130.216	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	66
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	66
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	65
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	64
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	64
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	63
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	61
79.182.124.209	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	58
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	50
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	50
213.8.173.129	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	49
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	49
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	48
79.178.181.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
31.154.145.96	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	44
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	44
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
176.13.10.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
2.52.46.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	41
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	41

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.142.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	253
79.183.211.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	234
89.138.75.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	192
46.19.86.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	182
89.139.185.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	152
149.50.73.48	United States	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	115
5.102.229.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	100
87.69.238.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
46.19.86.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
213.57.164.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
109.66.32.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
2.54.158.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
2.54.150.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
80.246.136.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	46
37.26.148.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
176.13.13.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
37.26.148.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
37.26.148.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
176.13.23.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	34
109.253.206.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	34
77.125.115.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
109.186.184.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
2.54.17.115	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	26
118.193.162.96	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 118.193.162.96	Block	25
2.54.148.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
176.13.17.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
109.65.169.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
89.139.73.190	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.139.73.190	Block	13
197.52.224.68	Egypt	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	12
5.102.228.9	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	12
197.52.224.68	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.52.224.68	Block	11
46.19.86.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
109.64.94.138	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/'	Block	11
2.54.41.68	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
5.102.228.9	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 5.102.228.9	Block	9
176.13.15.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
87.71.9.228	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	8
68.180.228.158	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/tmuna	Block	8
85.65.224.149	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 85.65.224.149	Block	8
87.71.9.228	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	8
197.52.224.68	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	7
197.52.198.220	Egypt	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	7
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
2.54.17.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
46.19.86.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
74.72.188.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
197.52.189.168	Egypt	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	6
197.52.128.201	Egypt	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	6
40.77.167.82	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6

03-12-2016 to 03-13-2016