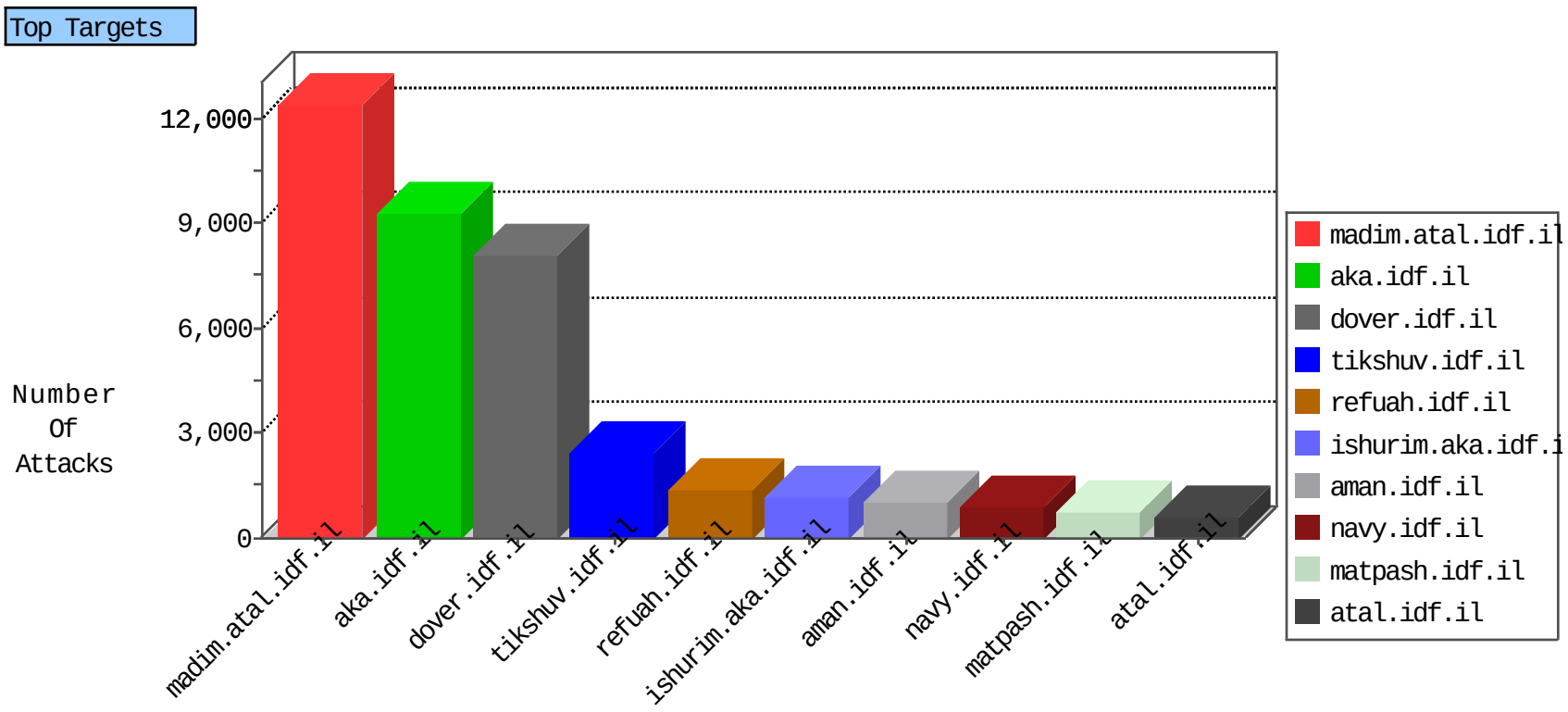
02-22-2016 to 02-23-2016

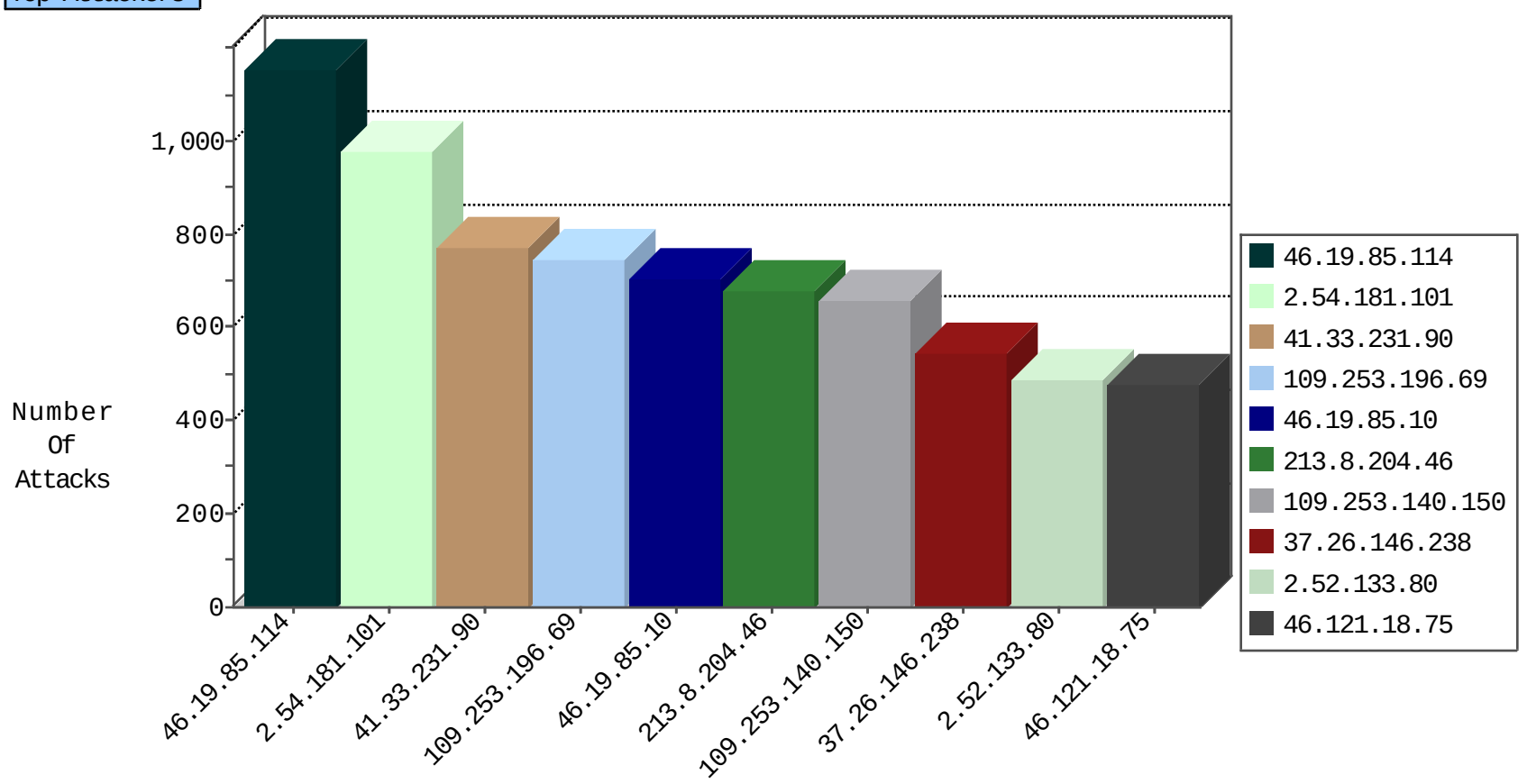
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-22-2016 to 02-23-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2882
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	778
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	316
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	253
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	200
204.93.154.210	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	197
212.179.34.170	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	194
204.93.154.200	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	193
37.26.148.222	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	142
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
194.165.146.149	Jordan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	50
37.26.146.241	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	21
2.54.17.253	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	10
109.65.112.60	Israel	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	9
190.151.178.4	El Salvador	147.237.8.24	e.lifestyle.idf.il	L4 Source or Dest Port Zero	drop	6
213.57.88.74	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	6
10.0.0.1		147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	5
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
31.131.4.153	Moldova, Republic of	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
8.37.71.78	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
31.168.225.146	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	3
79.182.25.186	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.76.39	mobile.meitav.idf.il	JLM_Purple_Con_Limit_Http	drop	3
31.168.240.21	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.179.46.189	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
207.46.13.127	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.178.112.202	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
40.77.167.98	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
141.0.14.147	Europe	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
31.154.27.186	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
183.60.48.25	China	147.237.76.34	yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
116.209.246.22	China	147.237.77.61	e.cogat.idf.il	Invalid TCP Flags	drop	2
79.182.25.186	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	2
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	2
141.0.14.147	Europe	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
8.37.231.199	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
221.231.6.167	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
185.130.5.201		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	2
193.242.218.6	Switzerland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
222.222.103.130	China	147.237.76.177	ncore.idf.il	Invalid TCP Flags	drop	2
115.239.228.10	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2

02-22-2016 to 02-23-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	41
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	41
80.246.130.210	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	30
106.120.173.130	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	22
79.179.34.222	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
149.78.6.246	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
64.31.44.3	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
149.88.223.106	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
5.29.212.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
217.132.152.229	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
212.179.132.203	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
79.182.162.129	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
136.243.5.215	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	10
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	9
109.65.219.9	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
89.138.173.26	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
109.67.22.33	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	8
193.106.206.10	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.177.119.239	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
31.168.144.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.160.147.209	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
37.26.146.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.181.18.17	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
91.106.46.6	Iraq	147.237.77.216	dover.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	8
177.185.194.92	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	8
64.31.44.3	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
93.173.235.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
74.208.133.60	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
184.168.193.34	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
84.108.237.163	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
62.210.170.165	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	8
177.185.194.92	Brazil	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
37.60.41.24	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
37.46.41.95	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
174.34.135.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	6
69.30.213.18	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	6
66.249.93.125	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.98	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.108.249.209	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.182.141.66	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
203.171.41.47	New Zealand	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
69.167.186.64	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
67.228.38.74	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
152.115.70.227	Denmark	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
94.159.159.90	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.137.81.122	Ireland	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
109.253.140.218	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4

02-22-2016 to 02-23-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	61
177.185.194.92	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	49
197.242.159.42	147.237.76.42	South Africa	refuah.idf.il	SQL Injection - Select From	28
64.31.44.3	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	26
74.208.133.60	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	20
108.168.219.174	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
184.168.193.34	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	14
46.137.81.122	147.237.76.86	Ireland	navy.idf.il	SQL Injection - Select From	14
217.70.44.165	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	13
66.96.128.60	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	13
69.167.186.64	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	12
152.115.70.227	147.237.77.74	Denmark	law.idf.il	SQL Injection - Select From	12
2.54.20.53	147.237.72.156	Israel	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	10
108.168.219.166	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	10
177.185.192.77	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	9
2.54.29.139	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	8
95.211.70.193	147.237.72.166	Netherlands	aka.idf.il	SQL Injection - Select From	7
67.228.38.74	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	7
46.137.81.122	147.237.77.233	Ireland	atal.idf.il	SQL Injection - Select From	6
209.173.241.141	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
94.73.145.90	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	6
202.124.109.87	147.237.77.74	New Zealand	law.idf.il	SQL Injection - Select From	6
80.246.133.212	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	4
37.26.146.238	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
203.171.41.47	147.237.77.74	New Zealand	law.idf.il	SQL Injection - Select From	4
221.139.14.120	147.237.77.216	Korea, Republic of	dover.idf.il	Tehila - Perl LWP with fake user agent	3
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	3
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	3
177.185.192.50	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	3
212.199.66.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
82.166.130.213	147.237.76.200	Israel	eitan.aka.idf.il	ET SCAN NMAP -sA (2)	2
84.111.76.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
81.218.241.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.81.236	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.81.139	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
212.179.155.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
46.60.77.237	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	2
212.179.79.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.64.159	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
194.90.25.122	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
212.33.112.140	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
87.69.95.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
211.23.251.92	147.237.77.74	Taiwan	law.idf.il	SQL Injection - Select From	2
66.249.93.103	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.233	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
81.218.130.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-22-2016 to 02-23-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	757
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	175
87.71.1.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	163
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	129
109.253.196.69	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	128
80.246.130.236	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	128
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	124
93.173.24.148	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	103
5.22.135.195	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
85.130.133.233	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	91
2.52.156.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
77.125.89.76	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	70
79.177.112.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
212.76.127.219	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	66
109.253.196.69	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	64
8.37.231.199	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	61
109.226.21.89	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
79.177.139.103	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	59
82.166.130.213	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	58
46.19.85.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52
212.76.127.10	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	48
2.52.132.0	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	45
46.116.75.52	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	41
212.76.127.111	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	39
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
5.102.242.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
31.210.188.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
41.254.2.37	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
31.210.188.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	37
23.80.148.170	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	37
23.81.247.58	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	37
109.253.138.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.52.9.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
77.126.51.108	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
46.116.151.131	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
46.19.85.141	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
2.52.39.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
212.76.127.44	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	33
23.81.247.225	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	32
194.156.44.7	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
2.52.42.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	31
23.80.148.11	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	31
80.246.136.4	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	31
2.52.168.102	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	30
109.66.211.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	29
188.247.77.187	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	28

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	951
2.54.181.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	886
213.8.204.46	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	680
109.253.196.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	552
46.19.85.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	514
109.253.140.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	462
46.121.18.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	434
2.54.130.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	368
37.26.146.238	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.146.238	Block	366
40.143.1.4	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 40.143.1.4	Block	342
109.253.206.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	334
2.52.133.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	311
46.19.86.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	299
109.253.159.108	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.159.108	Block	292
2.54.176.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	225
79.177.116.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	213
2.54.176.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	212
80.246.139.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	210
46.19.85.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	205
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	201
109.253.140.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	199
5.22.131.16	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	196
216.72.40.185	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	193
46.19.85.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	189
2.54.148.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	182
2.52.133.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	176
79.177.116.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	167
109.253.137.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	163
80.246.139.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	160
109.253.159.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	159
46.19.85.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	156
37.26.146.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	154
46.19.85.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	148
109.253.159.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	143
2.54.148.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	141
46.19.86.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	137
109.66.18.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	128
2.54.148.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	128
185.32.179.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	126
2.54.26.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	117
46.19.85.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	106
176.13.1.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	106
40.143.1.4	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	100
176.13.17.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	99
46.19.85.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	94
2.54.181.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	93
37.26.146.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	87
80.246.130.210	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	87
2.54.148.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
176.13.11.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	80

02-22-2016 to 02-23-2016