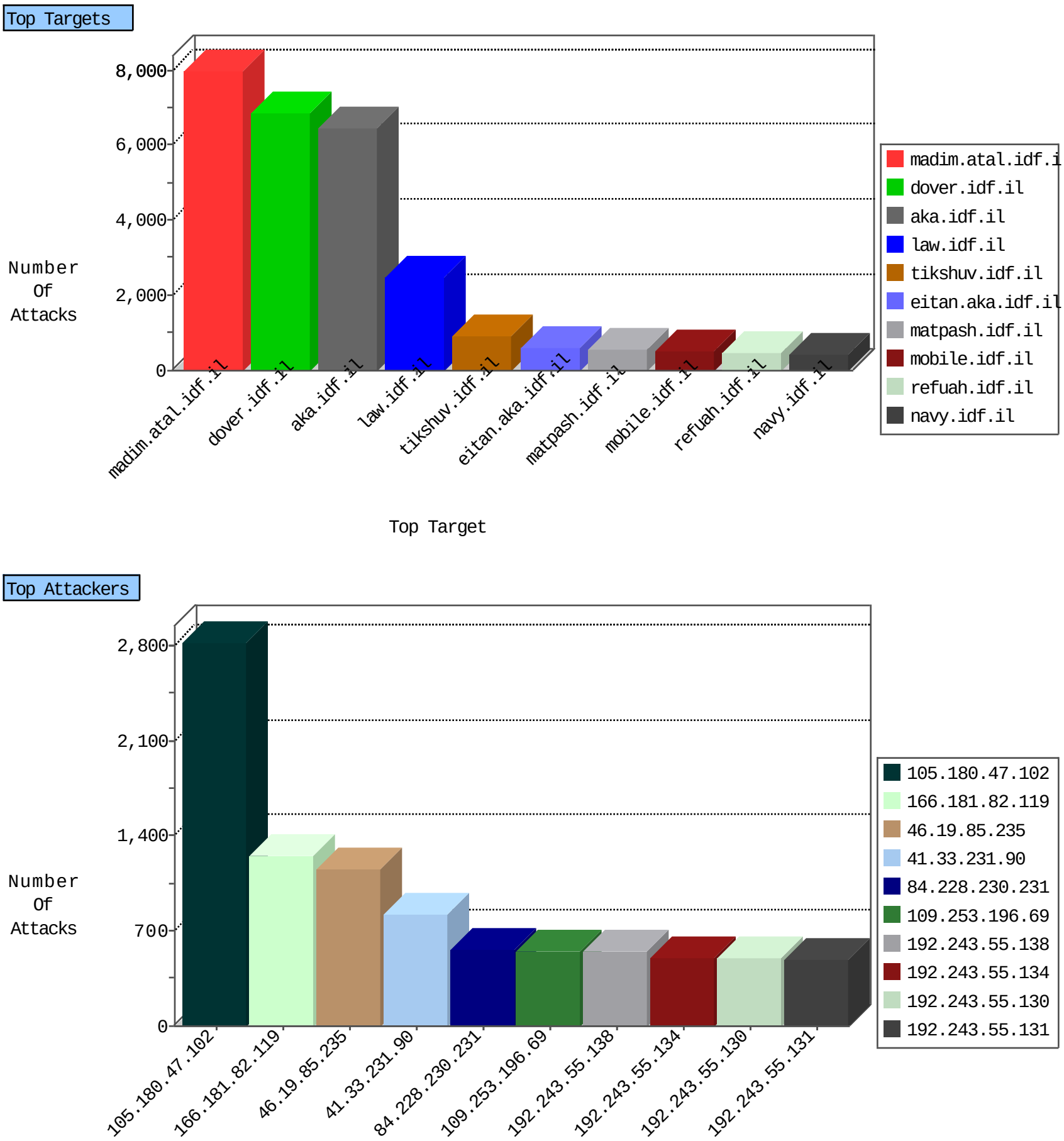
02-20-2016 to 02-21-2016

IDF Under Attack Daily Report



02-20-2016 to 02-21-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.243.55.130	Dominica	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3098
72.9.148.10	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3068
192.243.55.137	Dominica	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	278
105.107.51.229	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	137
79.183.13.52	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
66.249.69.34	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
217.172.189.11	Germany	147.237.76.30	himush.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	6
82.145.218.218	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
217.172.189.11	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	5
80.93.126.203	Ukraine	147.237.76.38	e.e.meitav.idf.il	L4 Source or Dest Port Zero	drop	4
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	4
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	4
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
80.93.126.203	Ukraine	147.237.76.197	e.himush.idf.il	L4 Source or Dest Port Zero	drop	3
112.121.190.17	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
185.130.5.201		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	3
80.93.126.203	Ukraine	147.237.76.147	chinuch.aka.idf.il	L4 Source or Dest Port Zero	drop	3
182.185.215.134	Pakistan	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	3
66.249.93.35	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3
185.130.5.201		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	3
112.121.190.69	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
82.80.25.198	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
112.121.190.9	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
112.121.190.70	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
185.130.5.201		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
82.132.229.15	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
112.121.190.10	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
95.27.15.125	Russian Federation	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
5.254.65.3	Romania	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3
112.121.190.71	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
185.130.5.201		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	2
185.130.5.201		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	2
183.60.48.25	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.239.228.10	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.130.5.224		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	2
41.251.65.109	Morocco	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
95.27.15.125	Russian Federation	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	2
218.247.180.3	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	2
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
8.37.227.163	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
121.199.23.158	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	2
208.100.32.119	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
80.93.126.203	Ukraine	147.237.72.217	e.idf.il	L4 Source or Dest Port Zero	drop	2
112.104.16.145	Taiwan	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	2
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2

02-20-2016 to 02-21-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	41
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	24
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	24
80.178.67.248	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	19
109.64.190.192	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	19
213.57.42.100	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	16
76.11.116.14	Canada	147.237.77.216	dover.idf.il	13912: HTTP: DirBuster Directory Enumeration Scanner	Block	16
46.121.81.86	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	13
5.22.135.102	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	11
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	11
46.19.86.212	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
10.0.0.9		147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
109.64.140.142	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	9
79.182.107.215	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
79.178.33.227	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
84.245.33.104	Netherlands	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
194.88.154.138	Poland	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
79.180.34.116	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
85.65.112.71	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
84.229.154.15	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
213.57.128.210	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
84.109.104.237	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
46.19.85.226	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	7
149.78.146.134	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
109.66.3.142	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
87.71.45.13	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
149.88.178.95	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
77.127.208.77	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
109.253.143.113	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
109.253.205.22	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
89.139.147.59	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
5.102.254.233	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
157.55.39.216	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	5
109.66.146.221	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	5
89.138.18.188	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	5
79.176.97.186	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	5
87.69.37.73	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
103.21.58.191	India	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
89.98.3.81	Netherlands	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	4
76.11.116.14	Canada	147.237.77.216	dover.idf.il	C1000067: HTTP: attempt to access .config page	Block	4
84.245.33.104	Netherlands	147.237.77.176	matpash.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
194.88.154.138	Poland	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
176.13.12.82	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
64.251.25.176	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
108.168.219.174	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.57.36.170	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
177.185.194.47	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
89.19.29.90	Turkey	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
89.138.105.117	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
84.108.238.169	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4

02-20-2016 to 02-21-2016

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	96
89.19.29.90	147.237.77.216	Turkey	dover.idf.il	SQL Injection - Select From	36
194.88.154.138	147.237.76.86	Poland	navy.idf.il	SQL Injection - Select From	36
188.120.148.137	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	30
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	18
84.245.33.104	147.237.77.176	Netherlands	matpash.idf.il	SQL Injection - Select From	18
69.167.186.64	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
64.251.25.176	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	12
64.251.25.176	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	12
108.168.219.174	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	12
177.185.194.47	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	10
178.63.18.196	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	6
103.21.58.191	147.237.77.233	India	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
64.87.23.55	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	6
66.249.93.97	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	4
162.216.19.183	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	3
5.102.254.122	147.237.76.86	Israel	navy.idf.il	INDICATOR-SCAN myscan	2
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
2.54.43.24	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
196.221.77.80	147.237.77.216	Egypt	dover.idf.il	SQL Injection - Select From	2
185.130.5.224	147.237.76.197		e.himush.idf.il	ET SCAN Potential SSH Scan	2
37.26.149.238	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
66.249.81.208	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	2
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.201	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
212.199.156.81	147.237.76.30	Israel	himush.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
66.249.75.215	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
109.253.205.234	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
188.161.37.37	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
5.102.254.233	147.237.0.34	Israel	tikshuv.idf.il	GPL SCAN myscan	2
5.102.254.122	147.237.76.86	Israel	navy.idf.il	GPL SCAN myscan	2
218.246.0.97	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	2
196.221.77.80	147.237.77.216	Egypt	dover.idf.il	GPL WEB_SERVER /etc/passwd	2
185.130.5.224	147.237.76.177		ncore.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.236	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
37.26.148.227	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
59.45.79.117	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.202	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	2
183.60.48.25	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	2

02-20-2016 to 02-21-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
105.180.47.102	Egypt	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2828
166.181.82.119	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1138
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	786
188.247.77.187	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	182
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	165
80.178.67.248	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	140
5.22.134.209	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	122
166.181.82.119	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	120
109.64.135.196	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
104.148.71.83	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	104
104.148.71.90	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	104
104.148.71.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	104
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
8.37.227.163	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	101
79.176.224.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	95
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	91
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	85
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	85
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	82
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	78
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	75
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	74
46.117.244.171	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	74
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	73
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	72
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	72
8.37.227.163	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	71
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	71
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	71
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	71
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	70
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	68
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	67
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	66
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	62
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	62
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	59
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	58
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	57
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	56
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	56
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	55
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	55
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	54
87.71.39.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
2.52.144.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
109.67.48.244	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	655
109.253.196.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	333
84.109.240.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	320
46.19.85.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	295
84.228.230.231	Bulgaria	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	287
46.19.85.109	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.109	Block	247
46.19.86.213	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.213	Block	243
37.26.148.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	234
109.253.196.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	194
85.250.102.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	186
84.110.109.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	182
84.228.230.231	Bulgaria	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	154
79.176.131.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	142
46.19.85.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	137
5.28.152.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	135
109.253.141.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	122
84.111.113.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	118
46.19.85.109	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.85.109	Block	117
84.109.240.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
84.110.109.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	113
109.253.141.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
176.13.6.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	108
79.176.131.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
2.54.153.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
37.26.149.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
85.250.102.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
84.228.230.231	Bulgaria	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
46.116.133.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	106
46.19.85.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
84.111.113.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
5.28.152.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.86.213	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	102
2.54.130.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	100
2.54.153.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	95
46.116.133.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	93
37.26.149.238	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.149.238	Block	82
79.179.96.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	82
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
89.139.139.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	73
176.13.2.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
79.182.198.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
2.54.53.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	71
46.19.85.235	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	69
2.52.16.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
176.13.6.119	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.6.119	Block	64
79.176.52.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
84.111.113.59	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 84.111.113.59	Block	62
85.250.102.236	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 85.250.102.236	Block	60
5.29.33.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	55