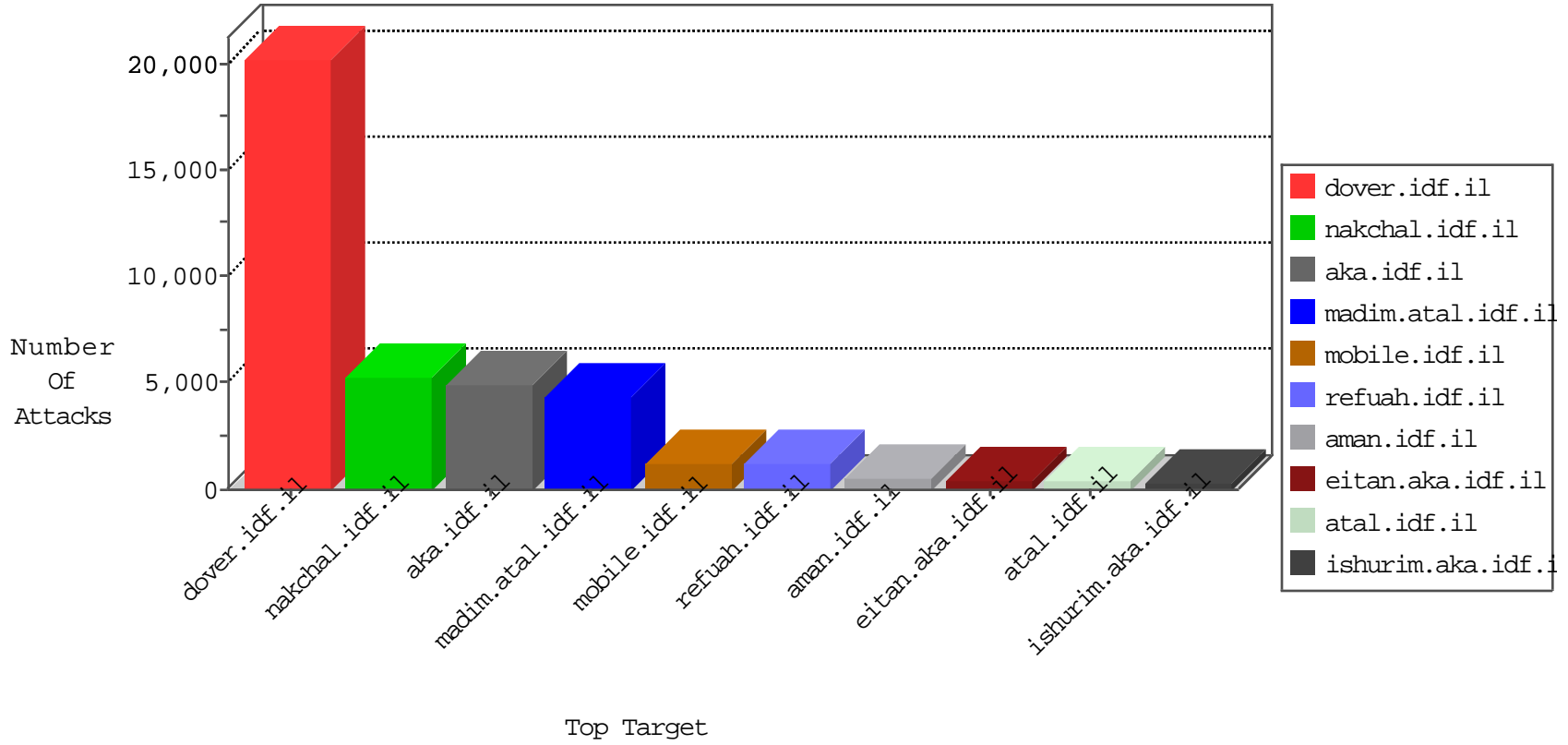


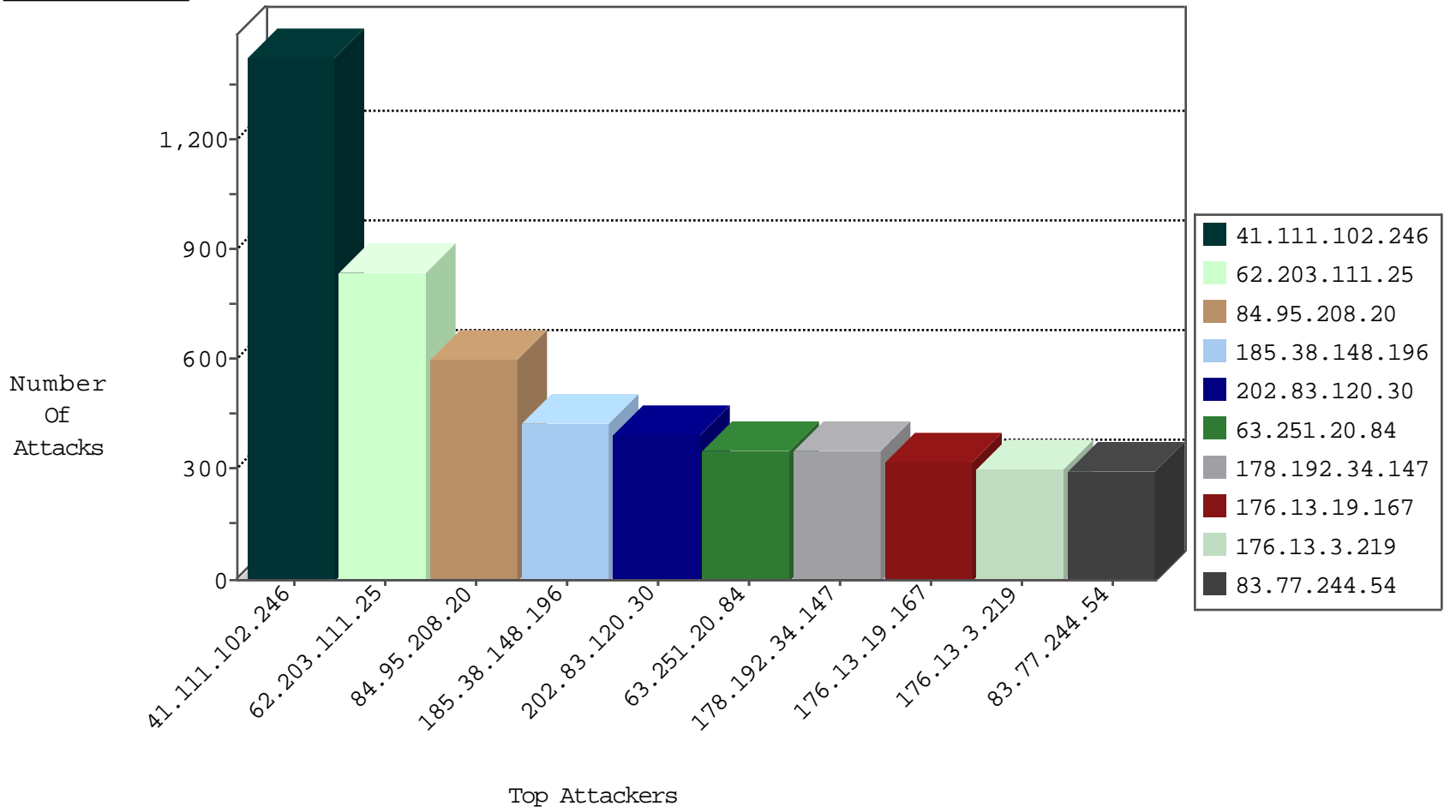
# IDF Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.231.57	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1224002
2.53.41.180	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4308
5.102.195.141	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1368
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-flooding	dest-reset	713
213.57.48.249	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	122
176.13.14.144	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32
2.55.186.171	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31
109.253.203.172	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
37.182.47.169	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
79.176.100.76	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
5.22.134.165	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
2.53.131.0	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
2.55.149.93	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
79.181.196.8	Israel	147.237.72.166	aka.idf.il	Black List	drop	9
176.13.237.193	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
31.168.204.250	Israel	147.237.77.216	dover.idf.il	Black List	drop	8
207.232.5.113	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
109.64.118.73	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.253.136.112	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
89.163.242.193	Germany	147.237.76.34	yochanan.idf.il	Black List	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
212.150.128.10	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
89.163.242.193	Germany	147.237.76.197	e.himush.idf.il	Black List	drop	5
89.163.242.193	Germany	147.237.76.199	e.nakchal.idf.il	Black List	drop	5
89.163.242.193	Germany	147.237.76.30	himush.idf.il	Black List	drop	5
2.53.5.85	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
89.163.242.193	Germany	147.237.76.201	e.atal.idf.il	Black List	drop	5
89.163.242.193	Germany	147.237.76.177	noore.idf.il	Black List	drop	5
217.65.35.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
2.53.169.108	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
31.168.204.250	Israel	147.237.72.167	ishurim.aka.idf.il	Black List	drop	4
2.53.141.74	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.53.147.88	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.53.45.19	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
89.163.242.193	Germany	147.237.76.39	mobile.meitav.idf.il	Black List	drop	4
199.203.108.177	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
132.72.78.122	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
89.163.242.193	Germany	147.237.76.86	navy.idf.il	Black List	drop	3
2.53.182.42	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
89.163.242.193	Germany	147.237.76.147	chinuch.aka.idf.il	Black List	drop	3
2.53.183.253	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
176.13.22.76	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
199.203.83.190	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
109.253.141.15	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
82.145.219.78	Europe	147.237.76.42	refuah.idf.il	Black List	drop	3
2.55.50.129	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
185.24.207.96	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
174.34.135.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	223
46.4.120.3	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	199
46.4.120.3	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	18
46.4.120.3	Germany	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	12
5.189.190.238	Germany	147.237.72.167	ishurim.aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	10
5.9.89.170	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	8
151.80.44.115	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	7
174.34.135.242	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	7
207.178.197.44	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
5.189.190.238	Germany	147.237.77.170	maarachot.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
5.189.190.238	Germany	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
5.9.89.170	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
174.34.135.242	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	4
144.76.29.66	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
144.76.29.66	Germany	147.237.77.226	www.chamatz.aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.4.120.3	Germany	147.237.76.147	chinuch.aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
123.126.68.103	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	3
108.59.8.70	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
31.43.128.9	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.9.89.170	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.189.190.238	Germany	147.237.72.167	ishurim.aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	2
104.223.17.50	United States	147.237.77.216	dover.idf.il	19791: HTTP: WordPress N-Media PHP File Upload	Block	2
46.4.120.3	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
163.172.220.113	United Kingdom	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
123.126.68.105	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
69.197.163.195	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.29.217.24	Israel	147.237.72.156	aman.idf.il	32390: HTTP: Suspicious User-Agent (Mozilla)	Block	2
213.251.184.38	France	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
71.13.87.122	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
240.0.10.13		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	2
151.80.44.115	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
93.174.95.106	Netherlands	147.237.76.176	test.ncore.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
69.30.213.202	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1
203.219.204.56	Australia	147.237.76.148	ggcenter.aka.idf.il	2226: Backdoor: TCP Window Size 55808 Trojan	Block	1
36.110.147.103	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
151.80.31.155	France	147.237.77.234	halag.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
37.26.148.247	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
151.80.31.175	France	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
104.223.17.50	United States	147.237.77.216	dover.idf.il	22611: HTTP: WordPress LoginWall Fake Plugin Usage	Block	1
5.189.190.238	Germany	147.237.77.170	maarachot.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
125.208.24.2	China	147.237.77.176	matpash.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
71.6.146.186	United States	147.237.77.179	e.mazi.idf.il	2226: Backdoor: TCP Window Size 55808 Trojan	Block	1
5.189.190.238	Germany	147.237.0.15	kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
151.80.31.183	France	147.237.72.156	aman.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
51.254.97.22	France	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.76.24	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	37
207.178.197.44	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	13
80.246.130.247	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	10
46.19.86.254	147.237.76.31	Israel	nakchal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	8
80.246.136.39	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
79.180.23.224	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	6
37.19.115.4	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	4
79.177.37.76	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	3
128.30.52.96	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.76.114	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
90.109.12.97	147.237.0.200	France	m4u.idf.il	ET SCAN Potential SSH Scan	2
46.120.122.219	147.237.77.176	Israel	matpash.idf.il	Xenu Link Sleuth User Agent	2
154.16.199.242	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	2
146.200.148.0	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
220.133.108.138	147.237.8.14	Taiwan	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
37.220.31.10	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	2
86.60.212.121	147.237.76.42	Finland	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
37.220.31.10	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	2
218.48.107.8	147.237.77.227	Korea, Republic of	e.hamaz.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
46.161.40.17	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
91.224.161.69	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
5.189.190.238	147.237.72.167	Germany	ishurim.aka.idf.il	ET WEB_SERVER Muieblackcat scanner	2
37.19.115.4	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
91.224.161.69	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	2
117.21.248.87	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
90.109.12.97	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
188.212.249.187	147.237.8.46	Romania	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
31.168.104.195	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
82.76.132.208	147.237.77.235	Romania	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
210.4.8.235	147.237.0.17	Philippines	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
86.90.10.151	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
186.72.87.70	147.237.8.45	Panama	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
218.88.235.154	147.237.77.205	China	prisha.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
93.171.33.219	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
84.108.67.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.208.165.101	147.237.72.217	Russian Federation	e.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.253.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
117.158.160.211	147.237.76.198	China	e.ychalan.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
211.144.82.140	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
79.180.189.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.162	147.237.76.86	China	navy.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
59.122.226.88	147.237.0.19	Taiwan	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
149.255.108.192	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.28.189	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.136.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.175.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.240.250.154	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	789
185.38.148.196	United Kingdom	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	414
63.251.20.84	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	342
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	208
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	195
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	192
66.227.185.95	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	176
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	171
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	156
125.235.240.171	Vietnam	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	124
62.0.207.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	123
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	121
195.212.29.181	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	112
109.65.189.108	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	111
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	100
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	99
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	98
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	85
196.53.36.190	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
32.211.172.47	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	81
68.43.98.16	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	81
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	81
173.61.255.101	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	76
50.83.49.57	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	75
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	74
80.246.130.194	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	74
172.56.35.244	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	73
40.131.136.215	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	68
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	68
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	68
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	67
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	64
79.181.18.233	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	62
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	61
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
2.53.159.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	59
62.0.212.209	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	56
162.253.131.35	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
193.47.165.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
207.46.13.79	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	50
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	49
213.8.204.43	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	48
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	46
68.131.64.241	United States	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.19.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	319
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 41.111.102.246	Block	301
176.13.3.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	278
176.13.14.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	250
185.32.179.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	224
46.19.85.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	197
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	189
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	181
185.120.125.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	181
37.26.146.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	170
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	142
5.29.110.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
37.26.146.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	125
80.246.137.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
109.253.201.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
2.53.129.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
46.19.86.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
31.168.115.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
176.13.238.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	89
37.26.148.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
109.253.219.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
2.53.183.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
46.19.86.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
176.13.20.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
176.13.16.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
46.19.86.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
2.55.141.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
37.26.146.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
37.26.148.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
2.53.10.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
109.253.192.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
46.19.85.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
37.26.146.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
37.26.149.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
2.55.168.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
2.55.178.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
2.53.15.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
84.108.65.217	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.65.217	Block	41
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	32
176.13.19.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
109.253.129.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
79.181.230.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
185.120.124.35	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.120.124.35	Block	25
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	25
46.19.86.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
95.86.104.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 95.86.104.235	Block	21
5.102.242.213	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.102.242.213	Block	18
109.253.200.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18