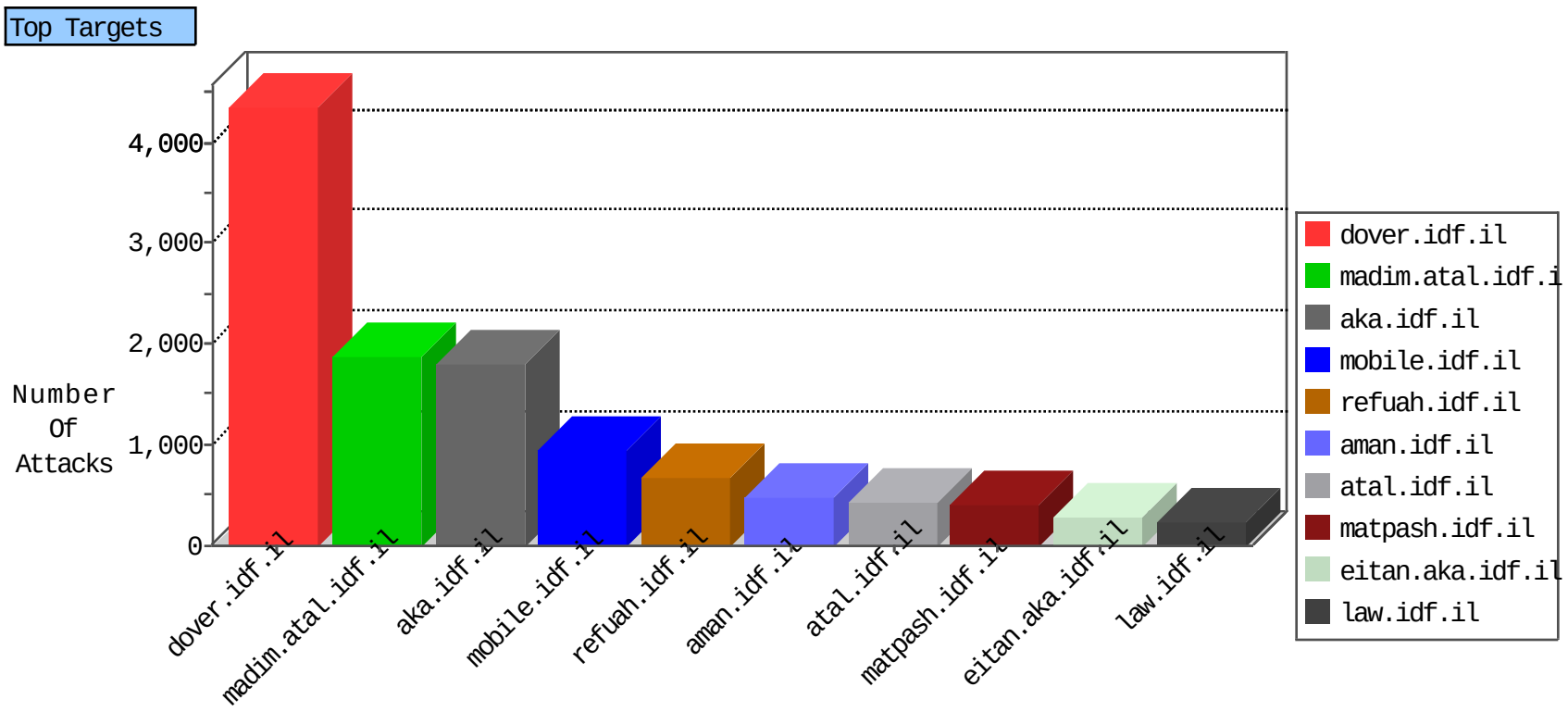
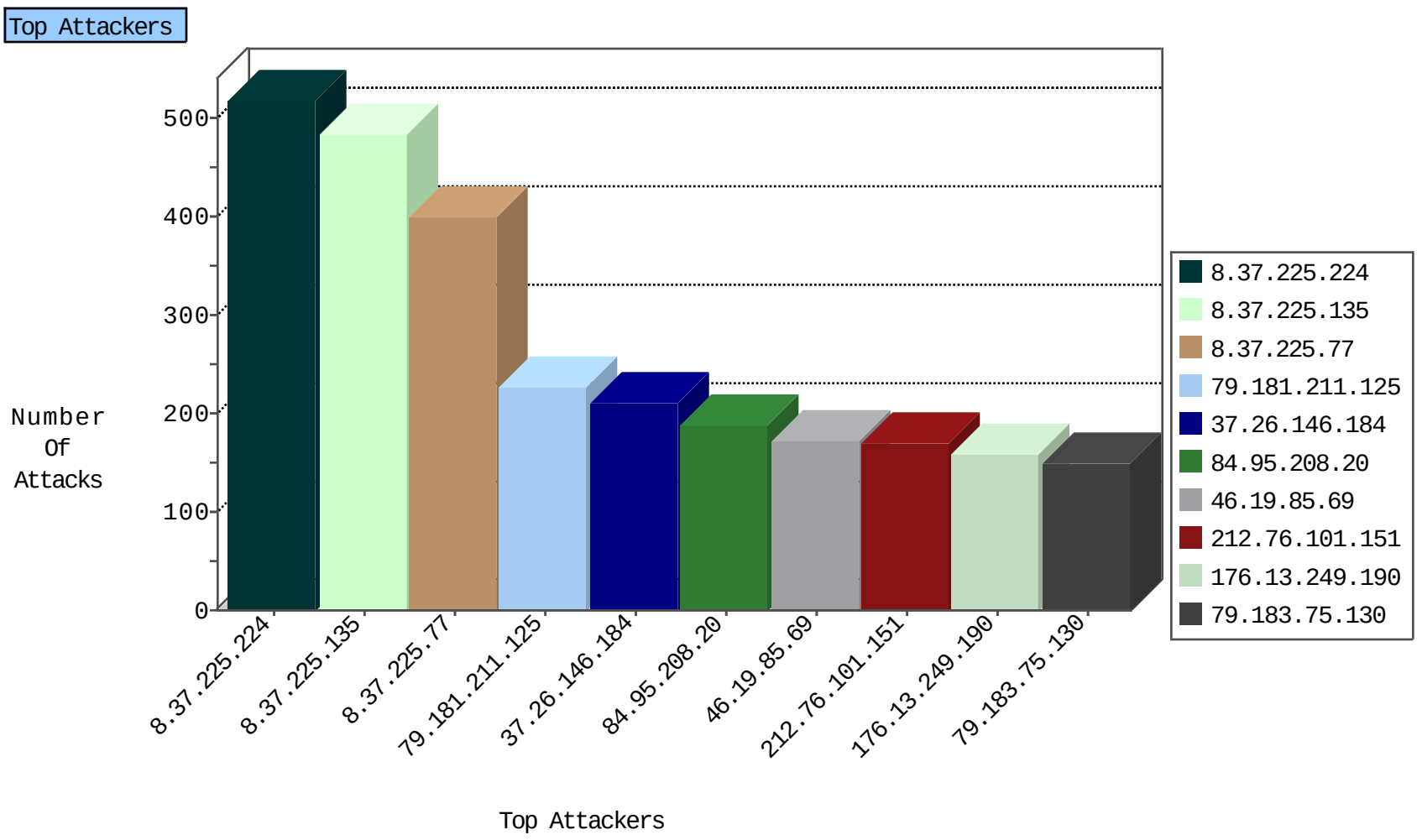
10-04-2016 to 10-05-2016

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-04-2016 to 10-05-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.201.142.53	Netherlands	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	22
185.89.217.233	Netherlands	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	21
8.37.225.77	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
83.249.181.44	Sweden	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	19
109.60.73.197	Croatia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	18
109.201.142.53	Netherlands	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	16
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	10
85.64.19.137	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
185.89.217.228	Netherlands	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	7
46.31.103.71	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
68.180.229.178	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
8.37.225.135	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
185.89.217.234	Netherlands	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5
95.86.100.91	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
207.46.13.141	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
8.37.225.135	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
8.37.225.77	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
95.86.80.20	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
8.37.225.77	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
95.86.80.20	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.181.211.125	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
8.37.225.224	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
82.145.219.92	Europe	147.237.76.86	navy.idf.il	Black List	drop	3
85.250.214.228	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
93.174.93.210	Netherlands	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
93.174.93.210	Netherlands	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	2
195.62.53.168	Russian Federation	147.237.77.233	atal.idf.il	block-sp-traf1	forward	2
195.62.53.168	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	2
221.229.172.116	China	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
93.174.93.210	Netherlands	147.237.77.234	halag.idf.il	block-sp-traf1	forward	2
93.174.93.210	Netherlands	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
204.12.217.4	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
93.174.93.210	Netherlands	147.237.72.156	aman.idf.il	block-sp-traf1	forward	2
69.30.193.253	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
63.141.231.196	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
195.62.53.168	Russian Federation	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
46.19.86.166	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
93.174.93.210	Netherlands	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
123.249.0.134	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
93.174.93.210	Netherlands	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
185.94.111.1	Russian Federation	147.237.76.31	nakchal.idf.il	Black List	drop	2
93.174.93.210	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	2
183.60.48.25	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
195.62.53.168	Russian Federation	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
222.186.34.148	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
93.174.93.210	Netherlands	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	2
190.230.147.253	Argentina	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
93.174.93.210	Netherlands	147.237.77.74	law.idf.il	block-sp-traf1	forward	2
204.42.253.130	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	2
93.174.93.210	Netherlands	147.237.72.166	aka.idf.il	block-sp-traf1	forward	2

10-04-2016 to 10-05-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.234.153.122	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	125
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	37
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	34
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	28
91.209.51.22	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	22
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	16
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	12
89.40.28.7	Romania	147.237.77.216	dover.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	10
89.40.28.7	Romania	147.237.77.216	dover.idf.il	22095: HTTP: Joomla Image Manager folderRename Security Bypass Vulnerability	Block	9
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	8
91.209.51.22	Ukraine	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	5
173.234.153.122	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	4
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
129.132.67.65	Switzerland	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	3
62.210.250.212	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
178.154.189.202	Russian Federation	147.237.77.216	dover.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	2
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.250.212	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.9.111.70	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.106	China	147.237.72.156	aman.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
173.234.153.122	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.148.247	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
178.154.189.204	Russian Federation	147.237.77.216	dover.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	2
162.210.196.129	United States	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.198.242	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
37.9.122.201	Russian Federation	147.237.77.216	dover.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	2
108.59.8.70	United States	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.247.125	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.254.129.90	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.106	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
198.245.49.215	Canada	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
173.208.157.186	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.255.194.3	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
89.98.142.25	Netherlands	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
178.154.189.201	Russian Federation	147.237.77.216	dover.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	2
162.210.196.97	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.250.212	France	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
198.245.49.215	Canada	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
173.208.157.186	United States	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Permit	2
54.187.255.228	United States	147.237.77.176	matpash.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
123.126.68.119	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
106.38.241.106	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
85.14.244.113	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1
193.111.140.106	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1
94.154.239.69	Ukraine	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	1
69.30.198.242	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	1
109.201.142.53	Netherlands	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
151.80.31.181	France	147.237.77.216	dover.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

10-04-2016 to 10-05-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.69.235	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	73
46.19.85.61	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	48
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	8
146.200.148.0	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	6
91.121.147.218	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
91.121.78.198	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	5
146.200.148.0	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	4
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	4
84.108.214.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	4
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	4
89.40.28.7	147.237.77.216	Romania	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.154.39.188	147.237.76.34	France	yohalan.idf.il	ET SCAN Potential SSH Scan	3
84.108.214.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	3
58.218.200.137	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
195.154.39.188	147.237.72.167	France	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	3
195.154.184.122	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
195.154.39.188	147.237.76.39	France	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
91.121.143.113	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
5.255.90.133	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	2
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
195.154.39.188	147.237.72.217	France	e.idf.il	ET SCAN Potential SSH Scan	2
222.186.56.200	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
87.163.134.17	147.237.0.33	Germany	idf.il	ET SCAN Potential SSH Scan	2
109.236.86.32	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
59.67.64.13	147.237.77.179	China	e.mazi.idf.il	GPL SCAN nmap TCP	2
62.210.124.129	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	2
195.154.53.146	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
109.236.86.32	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
195.154.39.188	147.237.0.200	France	m4u.idf.il	ET SCAN Potential SSH Scan	2
117.5.148.240	147.237.77.216	Vietnam	dover.idf.il	Xenu Link Sleuth User Agent	2
115.220.0.234	147.237.76.202	China	e.halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
208.100.26.228	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	2
195.154.39.188	147.237.0.19	France	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
195.154.39.188	147.237.76.42	France	refuah.idf.il	ET SCAN Potential SSH Scan	2
5.255.90.133	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	2
14.152.59.11	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
91.121.78.198	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
109.236.86.32	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
195.154.39.188	147.237.76.30	France	himush.idf.il	ET SCAN Potential SSH Scan	2
222.186.56.200	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	2
62.210.97.79	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
156.202.29.57	147.237.77.216	Egypt	dover.idf.il	ET WEB_SERVER Poison Null Byte	2
109.236.86.32	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
58.218.200.137	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	2
195.154.39.188	147.237.76.44	France	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
58.218.200.137	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
40.114.15.49	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.83.155.86	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1

10-04-2016 to 10-05-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.224	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	454
8.37.225.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	354
8.37.225.77	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	343
79.181.211.125	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	223
85.65.4.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	117
200.126.135.60	Argentina	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	109
79.180.95.145	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	108
141.0.12.30	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	97
66.249.65.53	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	90
79.180.8.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
8.37.225.224	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	62
77.127.4.101	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	60
2.53.54.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
8.37.225.135	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	57
79.183.75.130	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	57
8.37.225.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	55
79.183.75.130	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	54
46.31.103.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
8.37.225.77	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	49
141.226.218.10	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	45
5.29.190.82	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
109.66.58.1	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
77.126.4.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
213.6.75.166	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	36
83.130.246.83	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	34
79.183.75.130	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	34
2.53.39.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
5.22.134.99	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
77.125.21.0	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.55.39.152	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.163.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
141.226.162.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.28.113	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
46.19.86.197	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
46.43.88.223	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	24
1.39.25.210	India	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.119	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	23
187.61.127.153	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	23
107.167.106.35	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
46.19.85.20	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
46.19.86.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
176.13.230.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
134.196.125.83	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
107.167.109.199	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
107.167.117.19	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
107.167.109.145	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
141.0.13.88	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
185.89.217.225	Netherlands	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	211
212.76.101.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	170
176.13.249.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
46.19.85.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	146
37.26.147.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	132
2.53.143.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
176.13.18.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	86
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
2.53.155.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
176.13.242.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
37.26.148.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
84.108.232.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
85.64.17.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
79.180.14.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
46.19.86.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
37.26.148.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
116.24.250.26	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 116.24.250.26	Block	30
37.26.148.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
109.201.142.53	Netherlands	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.201.142.53	Block	27
46.19.86.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
37.26.148.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
176.13.20.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
84.109.102.53	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 84.109.102.53	Block	19
2.53.155.247	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 2.53.155.247	Block	19
116.24.250.26	China	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 116.24.250.26	Block	17
85.64.157.242	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.64.157.242	Block	17
116.24.250.26	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 116.24.250.26	Block	17
58.253.104.227	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 58.253.104.227	Block	17
175.44.19.5	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 175.44.19.5	Block	17
95.35.95.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	15
79.180.183.24	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.180.183.24	Block	14
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	13
217.132.148.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
116.24.250.26	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	11
87.69.247.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
82.166.240.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
46.120.122.219	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/726-en/patzar.aspx200oktext/html34445 idf law review 3200:00.359utf-8	Block	11
77.125.65.145	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	11
37.26.149.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
79.177.37.124	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	9
2.53.39.39	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
190.230.147.253	Argentina	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	8
190.230.147.253	Argentina	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/	Block	8
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	8
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	8
176.13.15.140	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.13.15.140	Block	7
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	7
46.19.85.28	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	7