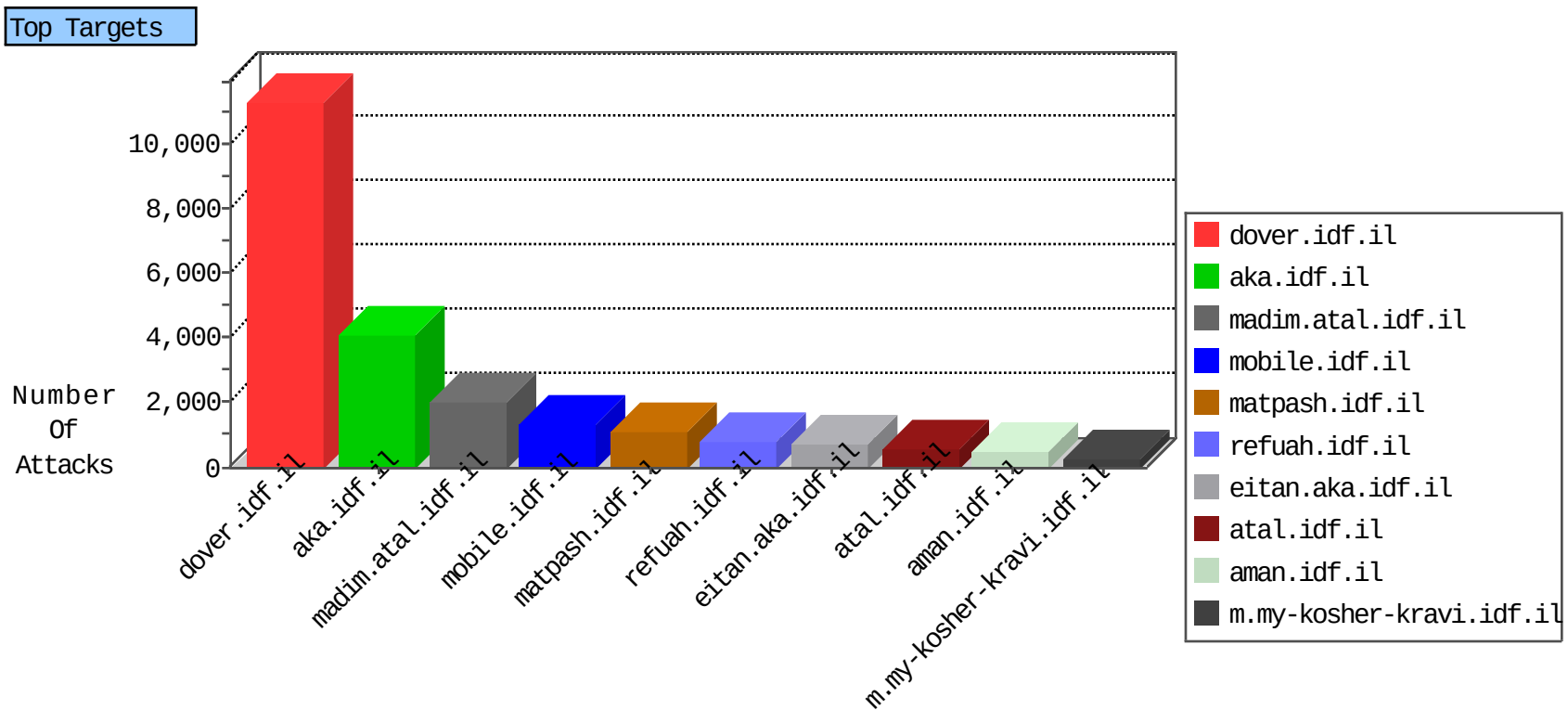
10-01-2016 to 10-02-2016

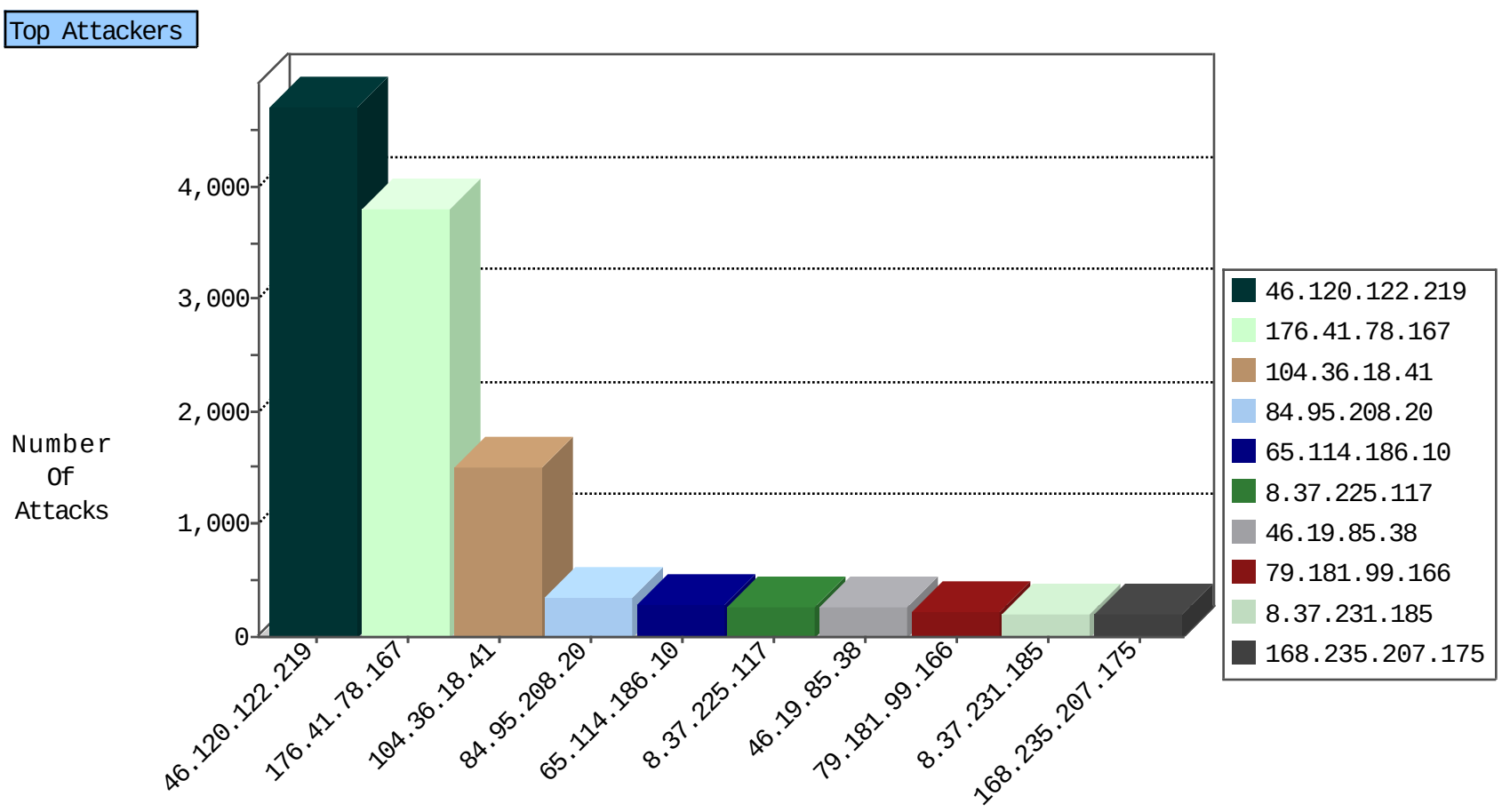
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-01-2016 to 10-02-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	4761
176.41.78.167	Turkey	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	forward	1437
176.41.78.167	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	579
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	442
176.41.78.167	Turkey	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	307
176.41.78.167	Turkey	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	92
104.36.18.41	United States	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	55
192.115.83.5	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	45
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	24
109.64.161.145	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	23
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	21
205.185.122.177	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
158.255.208.29	Hong Kong	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
217.148.44.140	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
109.64.161.145	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
176.111.109.155	Portugal	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
5.102.242.231	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	10
199.167.129.140	Canada	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
193.182.144.142	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
37.235.53.238	Spain	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
89.249.221.242	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
79.180.18.181	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
2.53.34.175	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
176.41.78.167	Turkey	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
176.41.78.167	Turkey	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
94.230.86.213	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
212.179.90.106	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	7
192.243.55.129	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
84.111.104.113	Israel	147.237.72.166	aka.idf.il	Black List	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
192.40.57.144	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	6
104.36.18.41	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	6
68.180.231.57	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
37.237.192.124	Iraq	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	6
104.36.18.41	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	6
8.37.225.117	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	5
192.71.249.215	Belgium	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
139.162.216.112	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
131.253.27.18	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.64.124.11	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
192.40.57.144	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
192.71.249.215	Belgium	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
109.253.214.101	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
158.255.208.29	Hong Kong	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
168.235.207.175	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3

10-01-2016 to 10-02-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.198.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	123
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	31
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	25
91.98.98.28	Iran, Islamic Republic of	147.237.76.42	refuah.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	17
46.4.123.172	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	17
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	15
46.4.123.172	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	10
69.30.198.242	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	6
23.91.70.94	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
158.85.253.245	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
108.175.157.102	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
72.167.131.75	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	6
201.216.208.137	Argentina	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.151.208.90	United Kingdom	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
158.85.253.245	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
174.47.99.30	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
74.208.230.195	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
202.124.109.87	New Zealand	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
64.34.186.9	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
158.85.253.245	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
23.91.70.43	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.172.106.100	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
137.117.9.67	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
46.118.155.156	Ukraine	147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	3
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
137.117.9.67	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3
125.64.94.206	China	147.237.0.34	tikshuv.idf.il	C1000003: HTTP: phpMyAdmin access	Permit	3
125.208.24.2	China	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	3
106.38.241.106	China	147.237.76.86	navy.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
108.59.8.80	United States	147.237.77.234	halag.idf.il	C1000074: HTTP: majestic bot	Permit	2
104.223.91.234	United States	147.237.72.156	aman.idf.il	32390: HTTP: Suspicious User-Agent (Mozilla)	Block	2
46.4.123.172	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
192.187.104.235	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.9.62.130	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.212.73.211	Netherlands	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.9.111.70	Germany	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
91.194.84.106	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
159.122.159.28	United States	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael - key words and groups	Permit	1
192.187.104.235	United States	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	1
91.98.98.28	Iran, Islamic Republic of	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
151.80.31.160	France	147.237.0.34	tikshuv.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.106	China	147.237.72.156	aman.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
151.80.31.108	France	147.237.76.147	chinuch.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

10-01-2016 to 10-02-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	1276
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	1143
46.120.122.219	147.237.77.176	Israel	matpash.idf.il	Xenu Link Sleuth User Agent	454
46.120.122.219	147.237.0.17	Israel	m.my-kosher-kravi.idf.il	Xenu Link Sleuth User Agent	255
46.120.122.219	147.237.76.200	Israel	eitan.aka.idf.il	Xenu Link Sleuth User Agent	157
66.249.65.21	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	156
46.120.122.219	147.237.76.86	Israel	navy.idf.il	Xenu Link Sleuth User Agent	126
46.120.122.219	147.237.76.42	Israel	refuah.idf.il	Xenu Link Sleuth User Agent	93
91.98.98.28	147.237.76.42	Iran, Islamic Republic of	refuah.idf.il	SQL Injection - Select From	54
46.120.122.219	147.237.0.34	Israel	tikshuv.idf.il	Xenu Link Sleuth User Agent	22
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	18
158.85.253.245	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	18
184.172.106.100	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
23.91.70.94	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	14
109.67.239.218	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	11
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	10
109.67.239.218	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	10
64.34.186.9	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
137.117.9.67	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
72.167.131.75	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
174.47.99.30	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
46.120.122.219	147.237.76.31	Israel	nakchal.idf.il	Xenu Link Sleuth User Agent	8
91.151.208.90	147.237.72.166	United Kingdom	aka.idf.il	SQL Injection - Select From	8
108.175.157.102	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
202.124.109.87	147.237.77.74	New Zealand	law.idf.il	SQL Injection - Select From	8
201.216.208.137	147.237.77.233	Argentina	atal.idf.il	SQL Injection - Select From	8
23.91.70.43	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
74.208.230.195	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
79.181.248.130	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	6
151.80.41.96	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
46.120.122.219	147.237.77.233	Israel	atal.idf.il	Xenu Link Sleuth User Agent	6
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	5
77.127.51.23	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	4
46.120.122.219	147.237.0.15	Israel	kosher-kravi.idf.il	Xenu Link Sleuth User Agent	4
66.249.65.51	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	3
183.60.48.25	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
46.243.112.156	147.237.77.226	Romania	www.chamatz.aka.idf.il	OS-WINDOWS Microsoft Windows RDP RST denial of service attempt	2
46.243.112.156	147.237.76.197	Romania	e.himush.idf.il	OS-WINDOWS Microsoft Windows RDP RST denial of service attempt	2
46.243.112.156	147.237.77.212	Romania	e.dover.idf.il	OS-WINDOWS Microsoft Windows RDP RST denial of service attempt	2
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	2
46.243.112.156	147.237.76.177	Romania	ncore.idf.il	OS-WINDOWS Microsoft Windows RDP RST denial of service attempt	2
103.208.244.223	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
46.243.112.156	147.237.77.179	Romania	e.mazi.idf.il	OS-WINDOWS Microsoft Windows RDP RST denial of service attempt	2
46.243.112.156	147.237.76.148	Romania	gqcenter.aka.idf.il	OS-WINDOWS Microsoft Windows RDP RST denial of service attempt	2
46.243.112.156	147.237.77.176	Romania	matpash.idf.il	OS-WINDOWS Microsoft Windows RDP RST denial of service attempt	2
103.208.244.223	147.237.0.19		madim.atal.idf.il	ET SCAN Potential SSH Scan	2
80.248.7.18	147.237.0.35	Nigeria	akaws.idf.il	ET SCAN Potential SSH Scan	2
46.243.112.156	147.237.76.86	Romania	navy.idf.il	OS-WINDOWS Microsoft Windows RDP RST denial of service attempt	2
46.243.112.156	147.237.77.121	Romania	e.navy.idf.il	OS-WINDOWS Microsoft Windows RDP RST denial of service attempt	2
46.243.112.156	147.237.8.27	Romania	e.madim.atal.idf.il	OS-WINDOWS Microsoft Windows RDP RST denial of service attempt	2

10-01-2016 to 10-02-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.41.78.167	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3449
104.36.18.41	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1223
176.41.78.167	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	228
104.36.18.41	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	215
8.37.225.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	202
168.235.207.175	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	191
84.111.64.141	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	182
65.114.186.10	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	175
176.228.144.37	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	152
109.65.149.210	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	124
141.212.121.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	120
8.37.231.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	117
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	109
2.53.53.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
46.19.86.187	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
184.175.54.173	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	87
168.235.197.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
8.37.231.185	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	77
65.114.186.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
77.127.74.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
217.132.51.228	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	66
8.37.225.117	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	65
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	63
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
85.65.4.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
176.228.165.205	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52
107.167.106.158	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	49
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	43
77.139.44.45	France	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
141.0.14.145	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
65.114.186.10	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
79.181.99.166	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	35
92.97.60.106	United Arab Emirates	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
50.79.101.141	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	34
2.53.2.130	Israel	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
141.0.14.217	Europe	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	32
46.19.86.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.180.22.50	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
213.8.204.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.251.119	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
212.143.186.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
79.182.105.109	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
87.169.64.66	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
192.115.83.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
172.56.16.140	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	24
2.53.184.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	23

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	995
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	260
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	235
176.13.13.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	166
109.253.208.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	153
2.53.157.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	149
109.253.223.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
79.178.43.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
79.180.46.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
84.94.58.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
109.253.196.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
109.253.144.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
109.253.147.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
46.19.86.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
37.26.149.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
46.19.85.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
14.127.67.88	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 14.127.67.88	Block	36
46.121.203.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
46.19.86.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
176.13.12.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
79.182.17.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
46.120.122.219	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.120.122.219	Block	26
77.139.102.129	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.102.129	Block	17
14.127.67.88	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 14.127.67.88	Block	16
46.19.86.22	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	16
2.53.157.234	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	14
31.154.81.40	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 31.154.81.40	Block	14
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	14
88.202.218.243	United Kingdom	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	14
80.246.139.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
37.26.149.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
14.127.67.88	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	13
46.120.122.219	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 46.120.122.219	Block	12
14.127.67.88	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 14.127.67.88	Block	12
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.122.219	Block	11
2.53.57.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	10
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	9
185.120.124.15	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	9
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	9
46.210.240.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.55.32.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	8
79.180.22.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
185.32.179.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
36.88.60.160	Indonesia	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	7
80.246.137.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
109.65.149.210	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	7