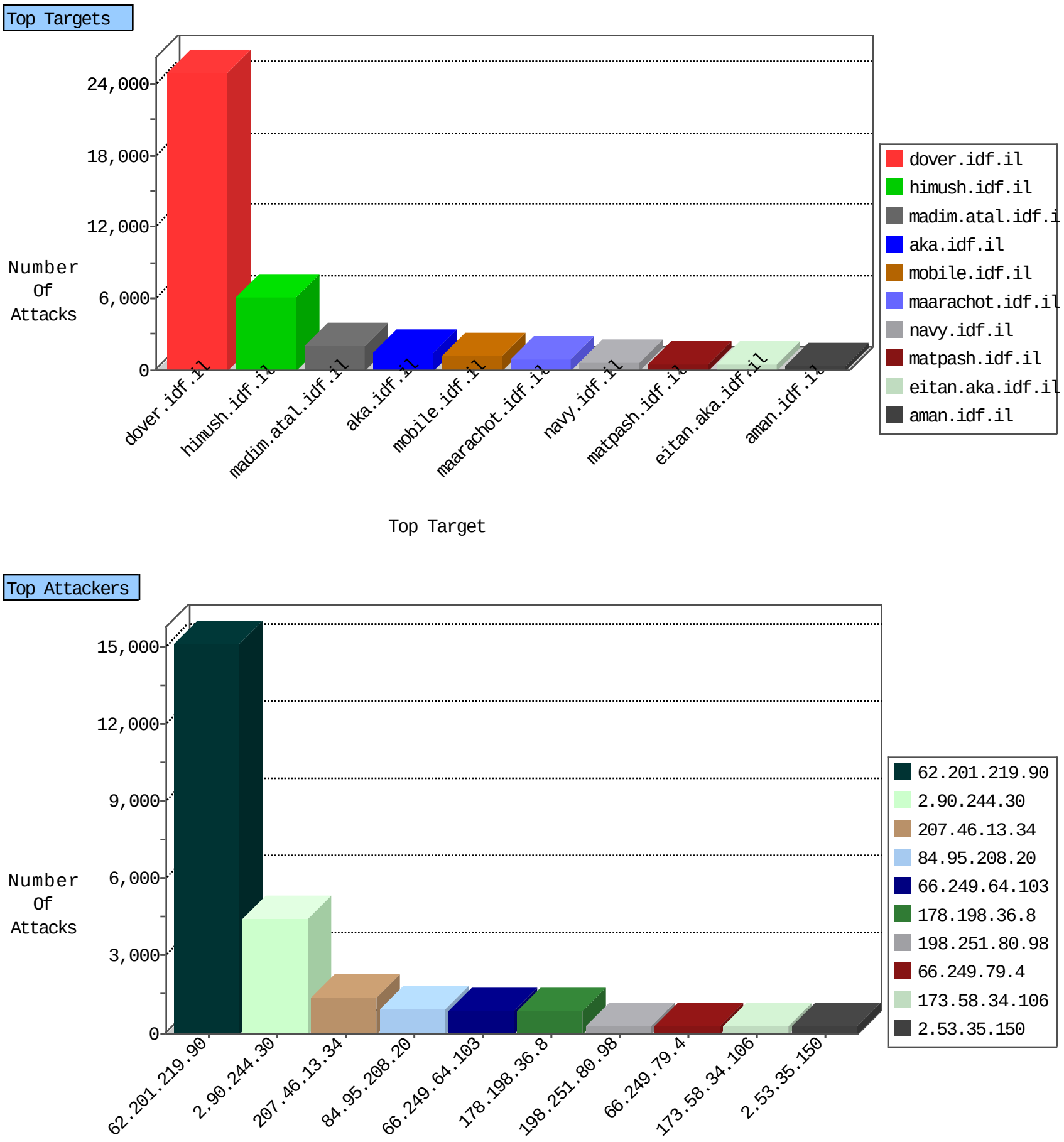
10-03-2016 to 10-04-2016

IDF Under Attack Daily Report



10-03-2016 to 10-04-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2986
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	55
2.90.244.30	Saudi Arabia	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	19
66.102.6.19	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
84.95.208.20	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
66.102.6.17	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
83.30.143.58	Poland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
46.19.85.49	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
2.90.244.30	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
50.87.144.145	United States	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	SYN Flood out of context	drop	4
2.53.37.105	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
66.249.65.51	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
180.160.34.245	China	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	3
66.249.85.179	Israel	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
8.37.231.152	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
79.177.88.21	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
185.94.111.1	Russian Federation	147.237.76.197	e.himush.idf.il	Black List	drop	3
89.248.163.3	Netherlands	147.237.76.34	yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
192.184.40.86	United States	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
209.126.136.2	United States	147.237.76.201	e.atal.idf.il	Black List	drop	2
77.139.192.75	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
93.174.93.218	Netherlands	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	2
195.62.53.168	Russian Federation	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
69.30.193.254	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
209.126.136.2	United States	147.237.76.30	himush.idf.il	Black List	drop	2
192.187.101.234	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
77.139.216.240	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
38.108.35.137	United States	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
93.174.93.218	Netherlands	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	2
85.250.214.228	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
192.187.109.59	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Black List	drop	2
209.126.136.2	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	2
105.107.99.2	Algeria	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
66.249.85.181	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
192.187.101.238	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
123.151.149.222	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
198.204.247.222	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
173.208.198.13	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
123.151.42.61	China	147.237.76.34	yohalan.idf.il	JLM_Under_Attack_Con_Udp	drop	2
209.126.136.2	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	2
106.38.241.106	China	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
209.126.136.2	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	2
195.62.53.168	Russian Federation	147.237.72.156	aman.idf.il	block-sp-traf1	forward	2
68.180.231.57	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
192.187.101.238	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2

10-03-2016 to 10-04-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.194.84.106	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	90
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	83
88.198.16.12	Germany	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	82
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	39
46.4.120.3	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	38
88.198.16.12	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	31
46.4.120.3	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	24
51.254.131.245	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	22
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	22
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	16
46.4.120.3	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	13
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	11
51.254.97.218	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	8
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	7
105.107.99.2	Algeria	147.237.77.216	dover.idf.il	12132: HTTP: BOIC DoS Tool	Block	6
37.113.61.0	Russian Federation	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	6
88.198.16.12	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	6
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	5
106.38.241.106	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	5
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	5
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
41.254.9.215	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	4
176.9.131.69	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	4
92.238.226.245	United Kingdom	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.4.123.172	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
176.9.131.69	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	3
51.254.131.245	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
51.254.141.46	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
69.30.221.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.4.32.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
178.151.143.163	Ukraine	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
144.76.4.148	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
88.198.16.12	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.9.8.150	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
178.151.143.163	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
151.80.41.169	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.254.141.46	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.106	China	147.237.76.86	navy.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
46.4.123.172	Germany	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
176.9.131.69	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.213.202	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
88.198.16.12	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.221.242	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.254.131.245	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.106	China	147.237.0.34	tikshuv.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
195.154.187.115	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.98	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.254.32.77	France	147.237.77.170	maarachot.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-03-2016 to 10-04-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.103	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	901
66.249.79.4	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	283
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	51
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	11
85.108.174.9	147.237.77.216	Turkey	dover.idf.il	Tehila - Perl LWP with fake user agent	10
62.219.165.221	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	6
91.121.143.113	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
91.121.184.8	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
146.200.148.0	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	6
80.246.130.47	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
84.108.214.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	4
41.254.9.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	SQL Injection - Select From	4
208.100.26.228	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	4
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	4
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.254.9.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	GPL WEB_SERVER /etc/passwd	4
117.5.148.240	147.237.77.216	Vietnam	dover.idf.il	Xenu Link Sleuth User Agent	4
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	3
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
208.100.26.228	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
208.100.26.228	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	2
62.210.113.216	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
91.121.142.199	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
208.80.155.222	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2
27.72.57.38	147.237.77.216	Vietnam	dover.idf.il	Xenu Link Sleuth User Agent	2
120.33.120.66	147.237.72.217	China	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
151.80.41.96	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
124.188.203.106	147.237.72.166	Australia	aka.idf.il	ET SCAN Potential SSH Scan	2
94.102.48.194	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	2
62.210.124.129	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
91.121.142.227	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
58.218.200.137	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
79.150.174.201	147.237.77.216	Spain	dover.idf.il	Xenu Link Sleuth User Agent	2
91.121.116.113	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
120.33.120.83	147.237.77.74	China	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
151.80.41.177	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
14.152.59.11	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	2
58.218.200.137	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
58.218.200.137	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
42.115.126.16	147.237.77.235	Vietnam	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
220.121.93.217	147.237.76.177	Korea, Republic of	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
14.152.59.11	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	2
162.250.190.142	147.237.77.216	Canada	dover.idf.il	Xenu Link Sleuth User Agent	2
139.162.13.205	147.237.77.226	Singapore	www.chamatz.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
2.55.141.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
101.24.189.34	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.120.95.250	147.237.76.39	Romania	mobile.meitav.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
178.79.141.130	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
14.177.180.2	147.237.77.205	Vietnam	prisha.idf.il	ET SCAN Potential SSH Scan	1
116.28.77.156	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-03-2016 to 10-04-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13948
2.90.244.30	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4331
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1368
173.58.34.106	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	272
193.41.165.8	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	267
66.249.65.53	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	221
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	185
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	183
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	173
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	171
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	160
185.3.147.193	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	154
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	150
176.13.230.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	150
77.126.4.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	141
86.84.54.34	Netherlands	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	141
8.37.231.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	141
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
63.143.224.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
198.251.80.98	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	91
176.13.3.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
66.150.121.194	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	88
213.140.59.130	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
198.251.80.98	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	79
198.251.80.98	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	78
192.225.253.33	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	77
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
77.127.12.244	Israel	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
24.251.78.5	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	67
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	66
115.28.218.121	China	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	65
109.235.254.148	Turkey	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	64
67.58.224.172	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	62
2.53.189.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
79.180.252.29	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
27.55.15.94	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
75.172.44.60	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	59
115.28.218.121	China	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	57
149.140.214.147	Turkey	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	57
115.28.218.121	China	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	57
74.105.148.193	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	56
66.151.138.9	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	54
67.8.44.143	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	53
24.4.50.221	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	53
105.107.99.2	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
8.37.231.152	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	49
24.4.50.221	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	49
24.4.50.221	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	48
24.4.50.221	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	47
213.140.59.130	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	47

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	428
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	Multiple Malformed URL from 62.201.219.90	Block	303
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 62.201.219.90	Block	303
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 62.201.219.90	Block	303
2.53.35.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	270
2.53.149.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	201
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	139
37.26.149.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	128
109.66.36.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
176.13.234.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	99
109.253.207.207	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	97
176.13.9.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
213.57.98.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
2.53.63.234	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	82
109.253.209.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 62.201.219.90	Block	68
194.242.165.42	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
2.53.173.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
176.13.224.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	33
77.127.12.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
85.65.190.124	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	31
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	28
46.117.253.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
37.26.147.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
46.117.128.137	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.117.128.137	Block	24
185.32.179.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
79.180.215.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	21
5.102.195.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
185.89.217.225	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
120.84.128.82	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 120.84.128.82	Block	18
109.65.77.29	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.65.77.29	Block	18
185.89.217.229	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.116.8.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
112.111.161.177	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 112.111.161.177	Block	17
185.89.217.227	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
120.84.128.82	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 120.84.128.82	Block	15
185.89.217.234	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
2.53.55.47	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.53.55.47	Block	15
185.89.217.232	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
185.89.217.230	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
185.89.217.228	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
79.178.13.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
87.71.54.34	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 87.71.54.34	Block	12
79.177.185.242	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	11
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	11
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	10
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	10