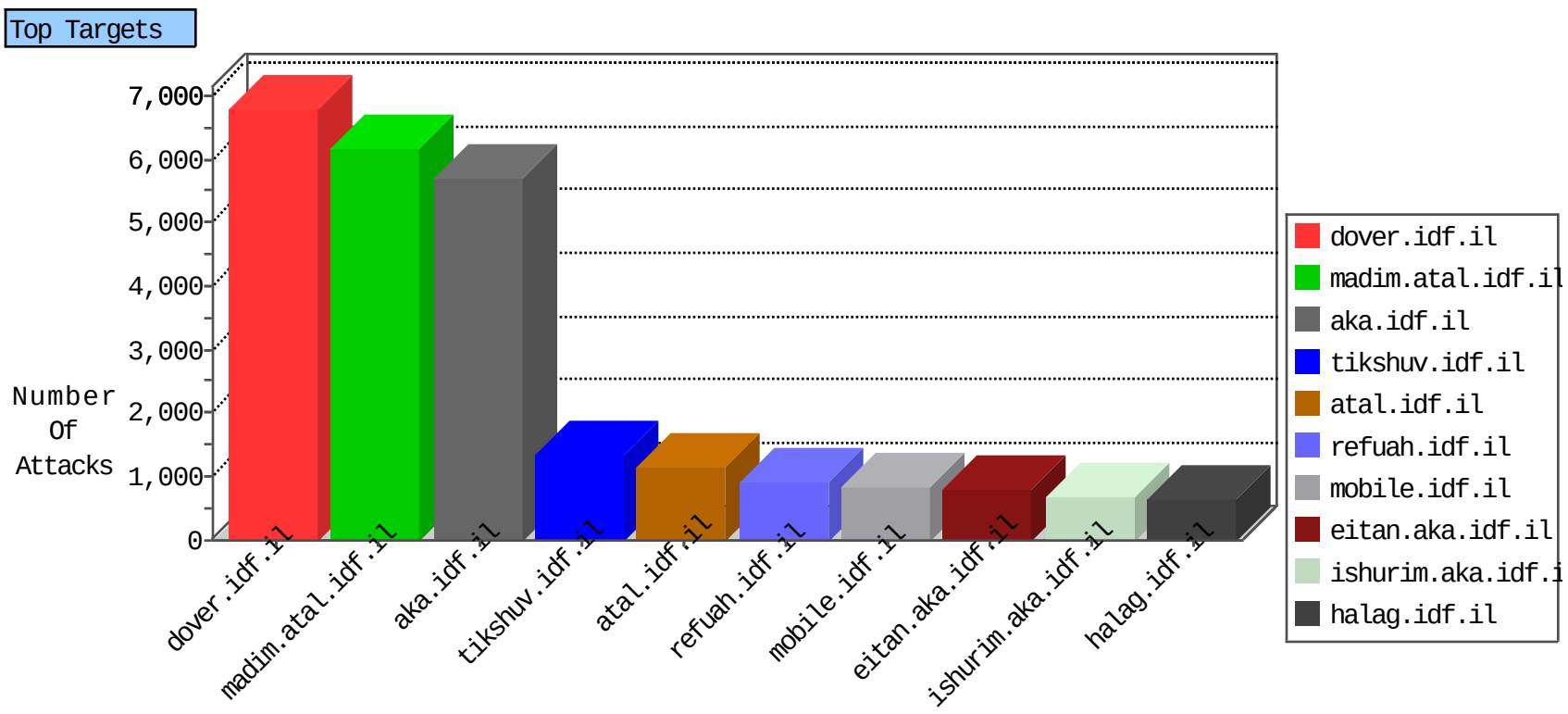
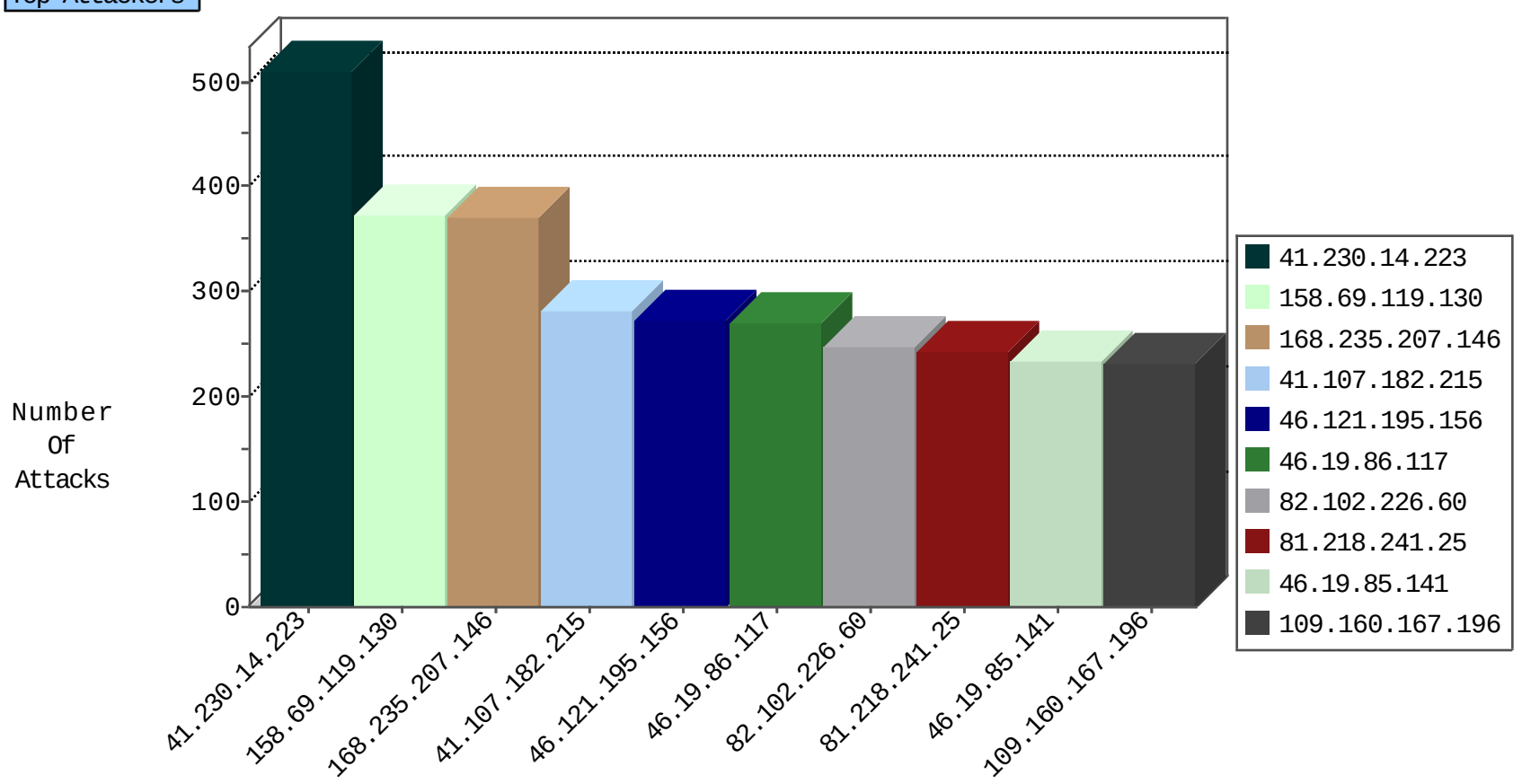
03-06-2016 to 03-07-2016

IDF Under Attack
Daily Report

Top Targets



Top Attackers



03-06-2016 to 03-07-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.107.182.215	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	4594
196.206.218.186	Morocco	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	2124
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	560
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	303
82.102.226.60	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	247
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	188
82.145.211.173	Europe	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	115
180.97.161.226	China	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	98
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	94
41.107.182.215	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	34
82.145.221.254	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	34
82.145.211.173	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	25
82.145.211.5	Europe	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	25
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	24
109.64.224.141	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	24
82.145.46.102	United Kingdom	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	23
82.145.218.61	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
82.145.219.147	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	11
37.26.149.195	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
109.67.143.233	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
87.70.242.235	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
82.145.209.96	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
212.199.34.114	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
2.54.19.212	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
46.19.86.53	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
2.54.190.110	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
105.156.29.17	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
62.219.224.99	Israel	147.237.77.234	halag.idf.il	Invalid TCP Flags	drop	6
79.177.186.18	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
31.168.232.150	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
82.145.209.222	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
109.253.146.58	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
82.145.217.125	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
62.0.104.195	Israel	147.237.77.233	atal.idf.il	L4 Source or Dest Port Zero	drop	5
134.147.203.115	Germany	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
199.203.136.47	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
176.13.7.104	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
66.249.64.190	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	3
5.28.174.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
93.172.147.82	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
176.13.1.52	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
2.54.143.43	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
46.19.85.72	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
84.108.236.54	Israel	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	3
192.118.132.185	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3

03-06-2016 to 03-07-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
158.69.119.130	United States	147.237.77.216	dover.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	36
158.69.119.130	United States	147.237.77.216	dover.idf.il	22095: HTTP: Joomla Image Manager folderRename Security Bypass Vulnerability	Block	35
31.168.232.154	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	28
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
61.135.189.108	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	20
5.102.206.148	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	18
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	16
82.166.141.45	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	16
85.64.56.193	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	12
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	12
84.111.82.147	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	12
80.246.130.34	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	12
109.67.143.198	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	12
81.218.251.252	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	12
80.246.130.171	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	12
79.183.204.199	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	11
79.182.201.167	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	10
207.46.13.70	United States	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	10
84.111.226.92	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	10
46.121.195.121	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	9
109.65.83.95	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	9
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	9
87.71.96.17	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.29.231.40	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	8
64.31.44.3	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
81.218.151.130	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.178.152.72	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.111.138.67	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.180.218.16	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.65.79.180	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	8
212.179.42.241	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	7
79.178.160.221	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	7
109.253.201.52	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	7
79.179.37.227	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	7
46.19.86.34	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	6
2.52.169.231	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.110.53.192	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	6
176.13.12.55	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	6
212.179.159.253	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	6
2.54.182.215	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	6
37.26.149.144	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	6
95.86.120.47	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	6
5.29.127.137	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	5
176.13.23.41	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	5
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	5
211.23.251.92	Taiwan	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
79.176.48.200	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.249.66.190	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	4
62.210.225.135	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
23.91.70.121	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

03-06-2016 to 03-07-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	134
158.69.119.130	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	90
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	66
186.84.183.121	147.237.77.216	Colombia	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	17
211.23.251.92	147.237.77.74	Taiwan	law.idf.il	SQL Injection - Select From	12
62.210.225.135	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	12
64.31.44.3	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	10
94.102.153.58	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	9
23.91.70.121	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	6
195.140.210.83	147.237.76.86	Germany	navy.idf.il	SQL Injection - Select From	6
89.38.209.50	147.237.0.34	Romania	tikshuv.idf.il	SQL Injection - Select From	6
209.15.196.171	147.237.77.233	Canada	atal.idf.il	SQL Injection - Select From	6
202.124.109.87	147.237.72.166	New Zealand	aka.idf.il	SQL Injection - Select From	6
66.135.63.82	147.237.77.226	United States	www.chamatz.aka.idf.il	SQL Injection - Select From	6
94.73.145.90	147.237.76.31	Turkey	nakchal.idf.il	SQL Injection - Select From	6
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
64.31.44.6	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
158.69.119.130	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	6
74.208.133.60	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
108.168.219.166	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	6
94.245.88.135	147.237.76.42	United Kingdom	refuah.idf.il	SQL Injection - Select From	5
217.70.44.165	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	4
66.102.8.243	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	4
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	4
66.249.64.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	4
216.249.107.200	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	4
212.199.216.2	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	3
218.246.0.97	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	2
212.179.155.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.64.34	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
218.57.11.7	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
94.102.48.193	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	2
218.57.11.7	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.121	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
198.54.90.200	147.237.77.233	United States	atal.idf.il	Tehila - Perl LWP with fake user agent	2
218.57.11.7	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
87.109.249.68	147.237.77.216	Saudi Arabia	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.69.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.196.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
188.213.219.175	147.237.72.167	Romania	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
117.34.70.143	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.230.93.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.241.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.77.19	United States	law-forum.idf.il	ET DROP Dshield Block Listed Source	1
61.244.49.137	147.237.76.200	Hong Kong	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.17.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
105.156.29.17	147.237.77.216	Morocco	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	1

03-06-2016 to 03-07-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.207.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	365
109.160.167.196	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	230
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	168
185.3.144.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	140
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	138
213.8.204.78	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	124
41.230.14.223	Tunisia	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	104
213.8.204.16	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	99
80.178.101.44	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	97
2.54.17.62	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
213.8.204.78	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	69
178.52.70.179	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	65
178.52.70.179	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	65
80.246.133.153	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	59
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
80.246.136.47	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
5.29.111.6	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
79.182.28.130	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
194.90.178.37	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	49
151.252.97.204	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	49
41.230.14.223	Tunisia	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	49
75.104.65.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
79.178.225.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
80.246.130.181	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	48
151.252.97.204	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	47
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	46
87.71.18.12	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
194.90.107.12	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
85.64.56.193	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	37
5.102.254.163	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	37
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	36
31.168.195.36	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
67.250.11.154	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.183.204.199	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.52.140.199	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
80.178.126.169	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
109.64.5.184	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.52.43.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.86.238	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.86.85	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
83.130.118.60	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
213.8.204.63	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
46.19.86.67	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	35
46.116.228.249	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
176.13.18.17	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33

03-06-2016 to 03-07-2016

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
87.71.35.164	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
212.179.21.194	Israel	147.237.77.212	e.dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	33

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.195.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	272
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	271
46.19.85.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	227
176.13.14.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	222
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	222
2.54.152.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	211
2.54.57.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	192
176.13.16.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	183
109.67.215.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	166
109.67.8.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	166
109.253.220.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	157
185.32.179.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	154
176.13.12.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
109.253.195.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
37.26.149.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	119
109.253.195.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
109.253.205.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
46.19.86.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
2.54.38.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
176.13.21.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	103
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	95
2.54.61.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
109.253.194.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
109.253.150.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
109.253.202.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
109.253.195.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
158.69.119.130	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	68
158.69.119.130	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 158.69.119.130	Block	68
2.54.128.16	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	67
185.32.179.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
2.52.40.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
176.13.16.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
2.54.154.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
176.13.12.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
75.104.65.29	United States	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 75.104.65.29	Block	58
109.253.212.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
46.19.86.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
46.121.27.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
80.246.136.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
176.13.15.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
2.54.33.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
176.13.8.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
80.246.137.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
46.19.85.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
80.246.136.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
2.52.10.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
80.246.139.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
2.54.179.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
2.54.151.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
93.173.39.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41

03-06-2016 to 03-07-2016