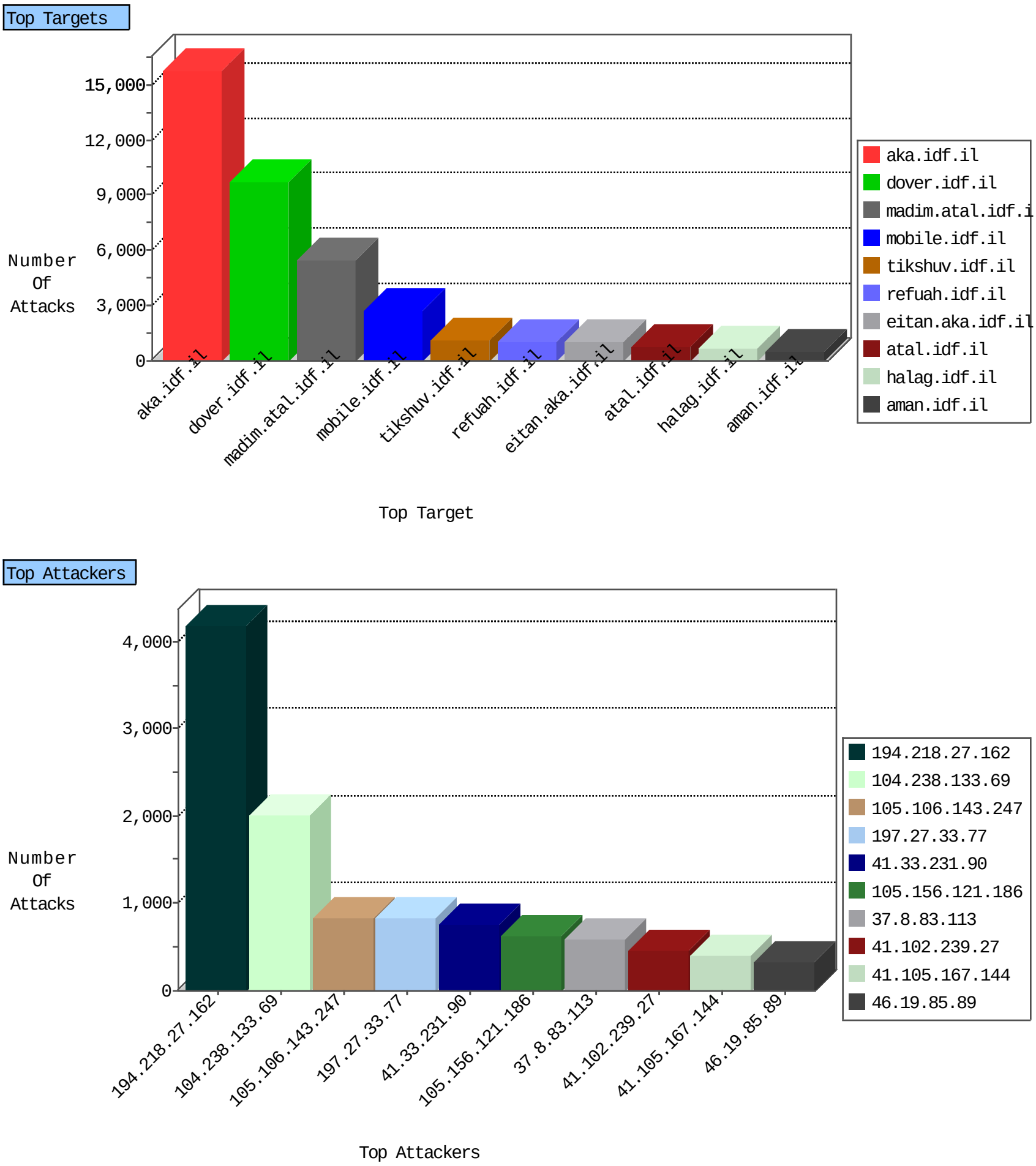
02-29-2016 to 03-01-2016

IDF Under Attack
Daily Report



02-29-2016 to 03-01-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	3848
104.238.133.69		147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2008
105.156.121.186	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	593
66.249.79.10	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	410
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	406
41.105.167.144	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	405
37.8.83.113	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	130
81.218.241.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	99
109.65.74.225	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	36
114.79.185.22	India	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	36
82.145.217.50	Europe	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	29
82.145.219.70	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	24
79.180.123.192	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	21
82.145.211.191	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	20
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	18
105.156.121.186	Morocco	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	17
82.145.219.82	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	14
79.180.123.192	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	14
217.26.171.188	Moldova, Republic of	147.237.76.176	test.ncore.idf.il	L4 Source or Dest Port Zero	drop	14
197.52.6.29	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	12
82.145.216.191	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	10
82.145.221.144	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
82.145.211.116	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
82.145.220.26	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	L4 Source or Dest Port Zero	drop	7
82.145.221.194	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
109.67.5.106	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
41.218.185.208	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
41.102.239.27	Algeria	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	6
82.145.219.83	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
109.65.224.142	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
87.79.69.115	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
82.145.217.94	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
31.210.186.254	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
82.145.222.181	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
58.176.20.99	Hong Kong	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	4
82.145.209.175	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	4
82.145.217.44	Europe	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	4
41.102.239.27	Algeria	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	4
79.182.233.69	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
84.110.209.192	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.180.12.103	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
84.110.209.192	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	3
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
93.80.161.65	Russian Federation	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Http	drop	3
192.118.132.185	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
70.39.185.66	Satellite Provider	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3

02-29-2016 to 03-01-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.127.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	50
193.43.245.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	32
193.43.246.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	30
46.116.28.23	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	22
61.135.189.110	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	22
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	21
31.154.41.13	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
106.120.173.124	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	20
79.178.192.226	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	19
2.54.165.234	Israel	147.237.72.166	aka.idf.il	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	18
2.54.159.176	Israel	147.237.72.166	aka.idf.il	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	17
79.183.152.62	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
176.13.13.248	Israel	147.237.72.167	ishurim.aka.idf.i	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	15
213.8.204.30	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
109.160.140.114	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
109.160.207.90	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
213.8.39.162	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	12
109.253.133.247	Israel	147.237.72.156	aman.idf.il	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	12
81.218.57.61	Israel	147.237.72.156	aman.idf.il	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	12
62.219.131.177	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	11
2.54.0.156	Israel	147.237.72.166	aka.idf.il	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	11
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	10
17.78.71.38	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	10
31.154.169.200	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
46.117.250.65	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
132.66.61.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
185.120.126.121		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
37.26.149.214	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
85.250.202.113	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.67.41.120	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
95.86.124.27	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
188.120.151.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.180.57.35	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
85.65.120.165	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.65.164.149	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
136.243.5.215	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	7
176.13.12.129	Israel	147.237.77.243	mobile.idf.il	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	7
2.54.168.72	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
212.199.71.118	Israel	147.237.72.166	aka.idf.il	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	7
80.179.203.49	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
85.65.167.150	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
89.139.135.114	Israel	147.237.72.166	aka.idf.il	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	6
212.179.42.241	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.177.51.42	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.179.127.175	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
82.80.198.164	Israel	147.237.77.216	dover.idf.il	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	6

02-29-2016 to 03-01-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.96	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	267
66.249.66.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	73
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	70
66.249.69.26	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	14
80.246.136.249	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
105.106.143.247	147.237.77.216	Algeria	dover.idf.il	ET SCAN NMAP -sS window 1024	5
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.64.163	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	5
66.249.66.81	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	4
80.246.130.20	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
109.67.190.134	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	3
105.106.143.247	147.237.77.216	Algeria	dover.idf.il	SQL Injection - Select From	3
174.37.194.144	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sA (2)	2
46.121.92.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
181.25.132.146	147.237.77.176	Argentina	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.10	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
46.19.86.238	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
82.221.48.130	147.237.76.42	Iceland	refuah.idf.il	Tehila - Perl LWP with fake user agent	2
79.180.61.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
82.166.152.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
46.19.85.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
66.249.64.180	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
84.109.12.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
80.246.133.30	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
109.66.152.145	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
66.249.64.153	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
37.26.149.199	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
213.8.204.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
94.102.48.193	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.66.90	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
2.52.140.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
66.249.66.36	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
109.253.131.186	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
132.74.95.21	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
212.29.203.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
2.54.181.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.52.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.249	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
79.181.144.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.235.254.181	147.237.76.176	Turkey	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.34.121	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.199.93.157	147.237.76.31	Costa Rica	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
81.218.57.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.64.189.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.210	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.44.133.108	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -f -sS	1
213.8.182.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-29-2016 to 03-01-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2796
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1399
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	726
41.102.239.27	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	311
197.27.33.77	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	306
37.8.83.113	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop		drop	212
80.178.197.104	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
37.8.83.113	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	154
87.71.49.36	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	150
37.26.146.133	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	141
79.180.123.172	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	132
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	132
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	117
94.252.183.68	Syrian Arab Republic	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	107
94.230.86.17	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	104
5.29.247.56	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	99
41.102.239.27	Algeria	147.237.77.216	dover.idf.il	drop		drop	97
212.25.69.22	Israel	147.237.76.200	eitan.aka.idf.il	drop	First packet isn't SYN	drop	93
70.39.185.66	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
94.252.183.68	Syrian Arab Republic	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	88
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	85
213.8.38.42	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	78
5.28.140.147	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	74
80.246.130.134	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	74
109.65.33.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
93.173.205.97	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	70
185.32.179.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
195.160.242.40	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	63
37.26.146.134	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
195.160.242.40	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	62
109.64.16.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	59
109.67.152.165	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	53
212.29.202.226	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	52
212.29.202.226	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	52
80.246.130.181	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	52
79.178.225.130	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
212.25.69.22	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
212.29.202.226	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	49
46.19.85.179	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
109.253.222.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
5.102.254.239	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
37.237.154.64	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	44
2.54.165.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
109.253.156.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
79.181.103.171	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
70.194.104.171	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
84.94.221.245	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38

02-29-2016 to 03-01-2016

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
37.8.83.113	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	38

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	330
109.67.24.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	236
2.54.162.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	212
46.19.86.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	187
80.246.136.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	183
37.26.149.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	181
197.27.33.77	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	173
109.253.211.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	173
2.54.18.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	168
109.253.213.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	150
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	148
109.253.192.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	143
46.19.85.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	142
109.253.147.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	142
46.19.86.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
37.26.149.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
176.13.6.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
109.253.137.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
46.19.85.71	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	116
46.19.86.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
176.13.18.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
80.246.136.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
84.108.51.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
37.26.149.162	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.149.162	Block	91
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
176.13.5.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
80.246.136.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
176.13.17.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
46.19.85.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
46.19.85.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
109.253.206.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
109.253.130.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
109.253.140.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
109.253.193.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
46.19.85.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
46.19.85.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
197.27.33.77	Tunisia	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	55
46.19.85.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
197.27.33.77	Tunisia	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	50
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
2.54.164.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
46.19.86.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
109.253.143.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
80.246.136.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
2.54.165.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
2.54.9.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
197.27.33.77	Tunisia	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	38
197.27.33.77	Tunisia	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	37
2.54.137.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36

02-29-2016 to 03-01-2016