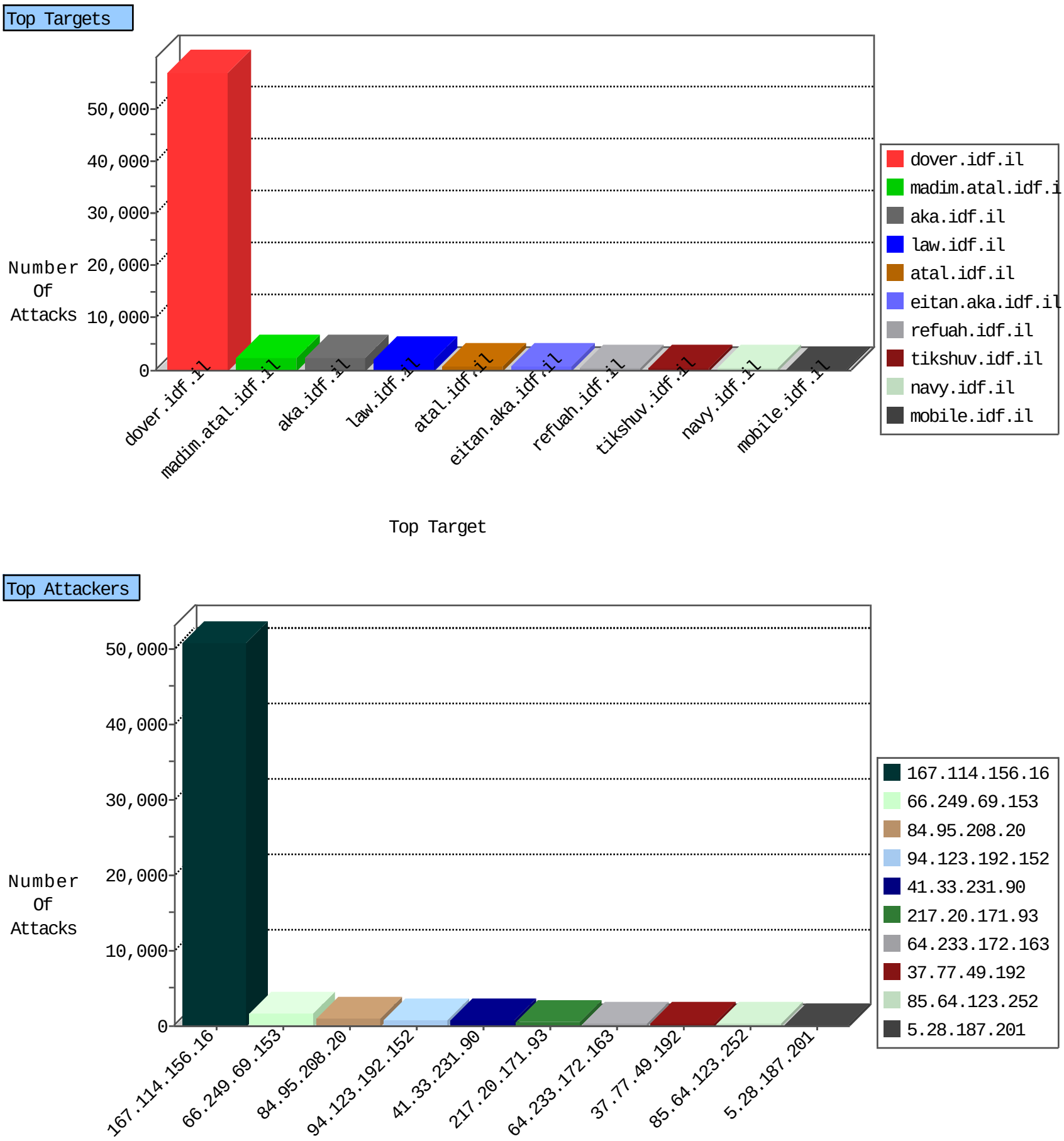
04-15-2016 to 04-16-2016

IDF Under Attack Daily Report



04-15-2016 to 04-16-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	50829
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	38
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	30
79.182.36.215	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	14
180.156.187.211	China	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	12
134.191.232.71	Israel	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Http	drop	9
79.180.198.74	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
84.108.174.55	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
79.178.217.205	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
37.144.87.226	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	6
79.177.39.89	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
84.108.152.18	Israel	147.237.72.156	aman.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
79.177.39.89	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
2.53.55.193	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
78.83.111.251	Bulgaria	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	4
37.144.87.226	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	4
120.132.50.135	China	147.237.77.233	atal.idf.il	block-sp-traf1	forward	4
125.127.86.131	China	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	3
79.180.198.74	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
203.189.74.44	Sri Lanka	147.237.77.176	matpash.idf.il	L4 Source or Dest Port Zero	drop	3
109.67.38.238	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
95.25.151.85	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
109.67.206.55	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	2
113.248.166.23	China	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	2
101.201.147.32	China	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	2
216.249.107.200	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
204.42.253.2	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
222.186.58.225	China	147.237.0.16	my-kosher-kravi.idf.il	JLM_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	2
120.132.50.135	China	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	2
204.42.253.2	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2
101.201.147.32	China	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	2
204.42.253.2	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	2
101.201.147.32	China	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
37.230.210.153	Russian Federation	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	2
95.25.151.85	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
204.42.253.2	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	2

04-15-2016 to 04-16-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	42
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	25
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	23
106.120.173.139	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	17
84.109.1.15	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
84.229.28.153	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
40.76.83.187	United States	147.237.0.17	m.my-kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	10
106.120.173.142	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	10
106.120.173.76	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	10
109.67.210.48	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
77.125.95.225	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
66.135.63.82	United States	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
109.65.19.225	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.117.233.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.66.23.97	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.180.58.71	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
77.124.24.35	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.183.60.212	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
40.76.83.187	United States	147.237.76.39	mobile.meitav.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
149.88.88.119	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
40.77.167.85	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
66.249.66.158	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
40.76.83.187	United States	147.237.76.30	himush.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
66.135.63.82	United States	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
46.4.123.172	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
67.228.38.74	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
173.234.159.250	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
37.26.146.177	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
216.249.107.200	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
195.234.228.90	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
79.179.113.100	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
176.13.7.157	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
94.102.153.58	United Kingdom	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
63.141.229.34	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
209.173.241.141	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
91.209.51.22	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
209.173.241.141	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
109.64.153.33	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
62.210.115.133	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
185.106.92.47	Russian Federation	147.237.76.30	himush.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	3
192.168.160.30	Israel	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	3
40.77.167.4	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
185.106.92.47	Russian Federation	147.237.77.234	halag.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	3
109.67.143.54	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
178.137.90.202	Ukraine	147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	3
66.249.66.162	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3

04-15-2016 to 04-16-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.69.153	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1590
64.233.172.163	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	402
66.249.66.114	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	188
66.249.78.29	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	155
66.249.78.89	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	104
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	96
66.135.63.82	147.237.77.226	United States	www.chamatz.aka.idf.il	SQL Injection - Select From	14
2.53.184.204	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	13
94.102.153.58	147.237.72.166	United Kingdom	aka.idf.il	SQL Injection - Select From	12
109.67.128.96	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	10
209.173.241.141	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	10
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
156.197.54.94	147.237.77.216	Egypt	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	8
94.73.150.148	147.237.76.42	Turkey	refuah.idf.il	SQL Injection - Select From	6
67.228.38.74	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
195.234.228.90	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	4
216.249.107.200	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	4
80.246.133.193	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
89.248.167.131	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
113.240.250.154	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.233	147.237.77.216	United States	dover.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
66.249.79.232	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
82.205.126.170	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	2
194.179.92.66	147.237.77.216	Spain	dover.idf.il	GPL SCAN nmap TCP	2
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
23.102.168.255	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
79.177.202.69	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
40.76.83.187	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	2
66.249.93.222	147.237.77.170	Europe	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.202	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sA (2)	2
91.201.236.155	147.237.77.170	Ukraine	maarachot.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
200.195.135.82	147.237.8.45	Brazil	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
80.82.78.38	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
177.207.143.25	147.237.0.33	Brazil	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
36.84.76.230	147.237.8.45	Indonesia	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.0.35	India	akaws.idf.il	ET SCAN NMAP -f -sS	1
104.44.133.108	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
88.204.187.90	147.237.8.45	Kazakstan	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
192.3.170.114	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
62.138.2.209	147.237.8.50	Germany	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
125.212.232.165	147.237.77.74	Vietnam	law.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.31.135	147.237.0.34	Japan	tikshuv.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection	1
13.92.100.128	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
107.158.255.194	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
96.127.95.81	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
220.179.172.185	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.76.31		nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.88	147.237.77.19	Lithuania	law-forum.idf.il	ET SCAN Potential SSH Scan	1

04-15-2016 to 04-16-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	740
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	568
217.20.171.93	Ukraine	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	356
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	294
5.28.187.201	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	206
217.20.171.93	Ukraine	147.237.77.74	law.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	195
93.172.168.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	149
95.24.151.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	130
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	125
197.132.189.201	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
176.77.14.16	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
95.26.49.207	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
95.220.187.53	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
110.92.98.4	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
5.22.131.57	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
80.246.130.146	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	58
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
5.144.60.235	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
176.193.108.13	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
37.144.87.226	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	44
23.27.45.25	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
176.77.86.62	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
176.13.17.181	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
89.139.177.97	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
178.140.124.201	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
207.241.229.187	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	40
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.67.249.193	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
213.57.60.209	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
101.128.179.75	Japan	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
178.140.87.205	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
109.63.145.137	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
123.126.113.101	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	25
89.108.144.116	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
79.180.238.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.67.174.13	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
94.197.120.163	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
46.19.85.120	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
89.108.144.116	Lebanon	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
176.13.17.181	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	21
46.19.85.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.37.14.115	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
37.237.210.135	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	20
37.237.210.135	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
2.53.171.72	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.13.13.192	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.123.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	246
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	221
80.179.30.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	172
149.78.215.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	167
89.138.211.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	160
46.19.85.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	159
37.77.49.192	Iraq	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.77.49.192	Block	148
37.77.49.192	Iraq	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 37.77.49.192	Block	139
2.53.185.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
176.13.8.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
37.77.49.192	Iraq	147.237.77.216	dover.idf.il	PHP Attempt	Block	101
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 94.123.192.152	Block	95
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Multiple Malformed URL from 94.123.192.152	Block	95
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 94.123.192.152	Block	95
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	89
176.13.17.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
176.13.6.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
213.151.35.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
37.26.149.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	72
46.117.198.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
46.120.142.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
109.253.142.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
46.121.112.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
109.253.142.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	48
46.19.86.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
37.26.149.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
109.253.138.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
5.189.190.212	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	35
79.177.233.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
37.26.149.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
5.22.130.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
176.13.21.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	25
37.26.148.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	17
176.13.11.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
2.53.63.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	14
37.26.146.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
46.19.85.56	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 46.19.85.56	Block	14
5.29.128.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
77.124.8.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
95.12.213.177	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.12.213.177	Block	11
2.53.164.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	10
40.77.167.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	9