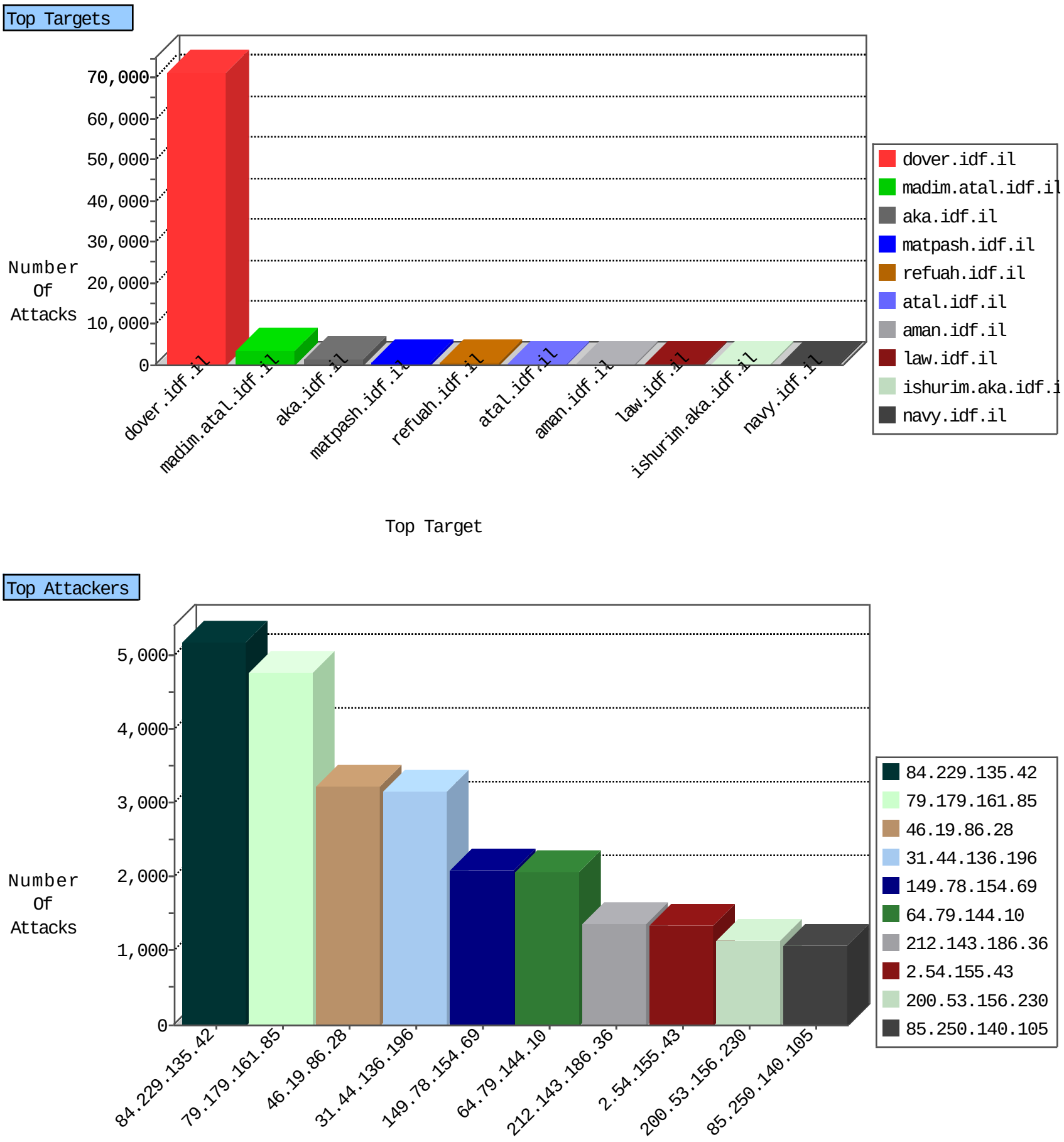
06-19-2015-00:00:02 to 06-20-2015-00:00:02

IDF Under Attack Daily Report



06-19-2015-00:00:02 to 06-20-2015-00:00:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
2.54.147.120	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6363
46.19.85.23	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	3852
200.53.156.230	Mexico	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2928
82.205.82.99	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2596
5.29.235.177	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	670
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	636
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	620
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	363
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	321
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	318
79.179.102.135	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	314
77.125.83.11	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	286
93.173.47.88	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	285
109.253.144.198	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	265
81.218.207.67	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	220
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	217
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
89.139.168.236	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	183
220.181.108.83	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	167
84.108.60.96	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	156
84.228.206.237	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	134
84.228.252.51	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	126
79.177.152.143	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
220.181.108.112	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	123
41.101.149.125	Algeria	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	121
85.250.117.65	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
84.110.86.51	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
79.177.135.116	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
93.172.156.62	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
212.199.218.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
46.19.86.133	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
109.64.132.210	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
85.65.46.68	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
109.65.102.119	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
77.127.84.240	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	76
79.179.49.181	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
149.88.203.229	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
2.54.181.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	74
79.180.183.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	70
109.64.154.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	70
37.142.99.241	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
79.178.33.15	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
79.177.152.143	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
84.108.60.96	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	forward	61
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	60
192.168.1.103		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
80.179.209.89	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
200.53.156.230	Mexico	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
79.179.62.197	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
66.249.81.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11

06-19-2015-00:00:02 to 06-20-2015-00:00:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
64.79.144.10	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	2067
109.64.111.70	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	214
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	168
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	148
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	144
173.208.136.26	United States	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
173.208.136.26	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
89.105.194.80	Netherlands	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	20
91.230.121.131	Ukraine	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	13
109.66.16.41	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
218.77.79.43	China	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	9
37.59.125.59	France	147.237.77.216	dover.idf.il	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	9
218.77.79.43	China	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	8
79.182.202.229	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
218.77.79.43	China	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	7
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	7
71.6.135.131	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	7
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	6
46.19.85.210	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
149.78.245.105	United States	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
80.178.146.96	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.135.131	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	6
188.138.9.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	5
218.77.79.43	China	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	5
183.60.217.62	China	147.237.76.197	e.himush.idf.il	DVRep_P-N_40-59	Permit	5
218.77.79.43	China	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	5
218.77.79.43	China	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5

06-19-2015-00:00:02 to 06-20-2015-00:00:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	138
66.249.65.45	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	86
2.54.149.150	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	20
66.249.67.76	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	6
185.32.178.167	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
66.249.78.159	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
176.31.105.124	France	147.237.76.31	nakchal.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.65.48	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.9	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	4
95.110.228.68	Italy	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
217.21.8.88	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
66.249.79.229	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	4
83.143.240.15	Europe	147.237.77.216	dover.idf.il	SERVER-WEBAPP JBoss JMX console access attempt	4
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
43.255.188.132	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	3
83.143.240.15	Europe	147.237.77.216	dover.idf.il	ET WEB_SPECIFIC_APPS Possible JBoss JMX Console Beanshell Deployer WAR Upload and Deployment Exploit Attempt	3
83.143.240.15	Europe	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible CVE-2013-0156 Ruby On Rails XML YAML tag with !ruby	2
43.255.188.132	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.137	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
83.143.240.15	Europe	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_proxy reverse proxy information disclosure attempt	2
83.143.240.15	Europe	147.237.77.216	dover.idf.il	ET SCAN Apache mod_proxy Reverse Proxy Exposure 1	2
83.143.240.15	Europe	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	2
43.255.188.131	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
83.143.240.15	Europe	147.237.77.216	dover.idf.il	WEB-FRONTPAGE /_vti_bin/ access	2
43.255.188.130	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
82.205.45.119	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	2
85.250.140.105	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.84.208	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.183.128.6	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.131	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.64	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.144	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.131	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
83.143.240.15	Europe	147.237.77.216	dover.idf.il	ET SCAN Apache mod_proxy Reverse Proxy Exposure 2	2
43.255.188.130	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.162	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.133	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
83.143.240.15	Europe	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	2

06-19-2015-00:00:02 to 06-20-2015-00:00:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.229.135.42	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5195
79.179.161.85	Israel	147.237.77.216	dover.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	4700
46.19.86.28	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3232
31.44.136.196	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3164
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2108
212.143.186.36	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1375
2.54.155.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1356
85.250.140.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1082
2.54.147.120	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1026
46.19.85.40	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	937
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	667
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	650
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	632
200.53.156.230	Mexico	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	609
37.142.110.218	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	602
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	590
15.203.233.78	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	514
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	496
212.179.42.225	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	452
141.0.15.211	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	415
5.29.242.147	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	392
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	384
176.65.11.76	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	371
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	359
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	339
203.116.187.1	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	325
84.94.32.197	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	320
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	312
94.29.130.107	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	312
54.187.55.213	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	300
89.108.148.146	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	299
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	284
5.255.253.33	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	283
37.238.136.18	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	281
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	273
200.53.156.230	Mexico	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	273
66.249.93.164	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	253
66.249.93.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	251
66.102.8.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	235
68.180.229.51	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	231
197.28.71.119	Tunisia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	225
66.249.93.160	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	213
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	211
93.173.152.113	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	208
37.48.32.243	Czech Republic	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	204
83.143.240.15	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	198
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	197
188.161.246.23	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	190
66.102.8.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	190
66.102.8.178	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	184

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
149.78.49.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	849
84.108.219.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	615
185.32.178.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	343
85.250.27.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	304
2.52.166.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	276
89.139.54.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	209
109.160.137.11	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.160.137.11	Block	196
2.54.50.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	185
109.253.139.177	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.139.177	Block	125
176.65.11.76	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 176.65.11.76	Block	95
176.65.11.76	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	94
2.54.148.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	84
185.32.178.167	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.178.167	Block	82
79.179.49.181	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.179.49.181	Block	80
176.12.145.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	73
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	48
200.53.156.230	Mexico	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	35
37.26.147.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	25
109.64.183.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	20
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	20
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	18
68.180.229.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.229.51	Block	17
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	14
109.65.202.63	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	14
46.117.51.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
5.102.199.82	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.102.199.82	Block	13
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	12
46.121.125.224	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	11
93.173.40.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
212.199.142.58	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	9
79.176.154.44	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	9
2.54.182.179	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.182.179	Block	9
109.65.202.63	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	8
213.57.154.162	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 213.57.154.162	None	7
104.250.147.218		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
197.160.69.201	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	7
94.230.86.142	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	6
85.64.121.84	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 85.64.121.84	Block	6
31.13.100.115	Ireland	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
109.64.97.120	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	6
197.160.194.246	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
92.99.195.125	United Arab Emirates	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
41.46.202.3	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	5
87.68.52.82	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	5
197.160.69.201	Egypt	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	5
197.33.119.171	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.33.119.171	Block	5
85.64.121.84	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	5
69.160.54.33	United States	147.237.77.170	maarachot.idf.il	Suspicious Response Code	Block	5
93.173.60.233	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5

06-19-2015-00:00:02 to 06-20-2015-00:00:02