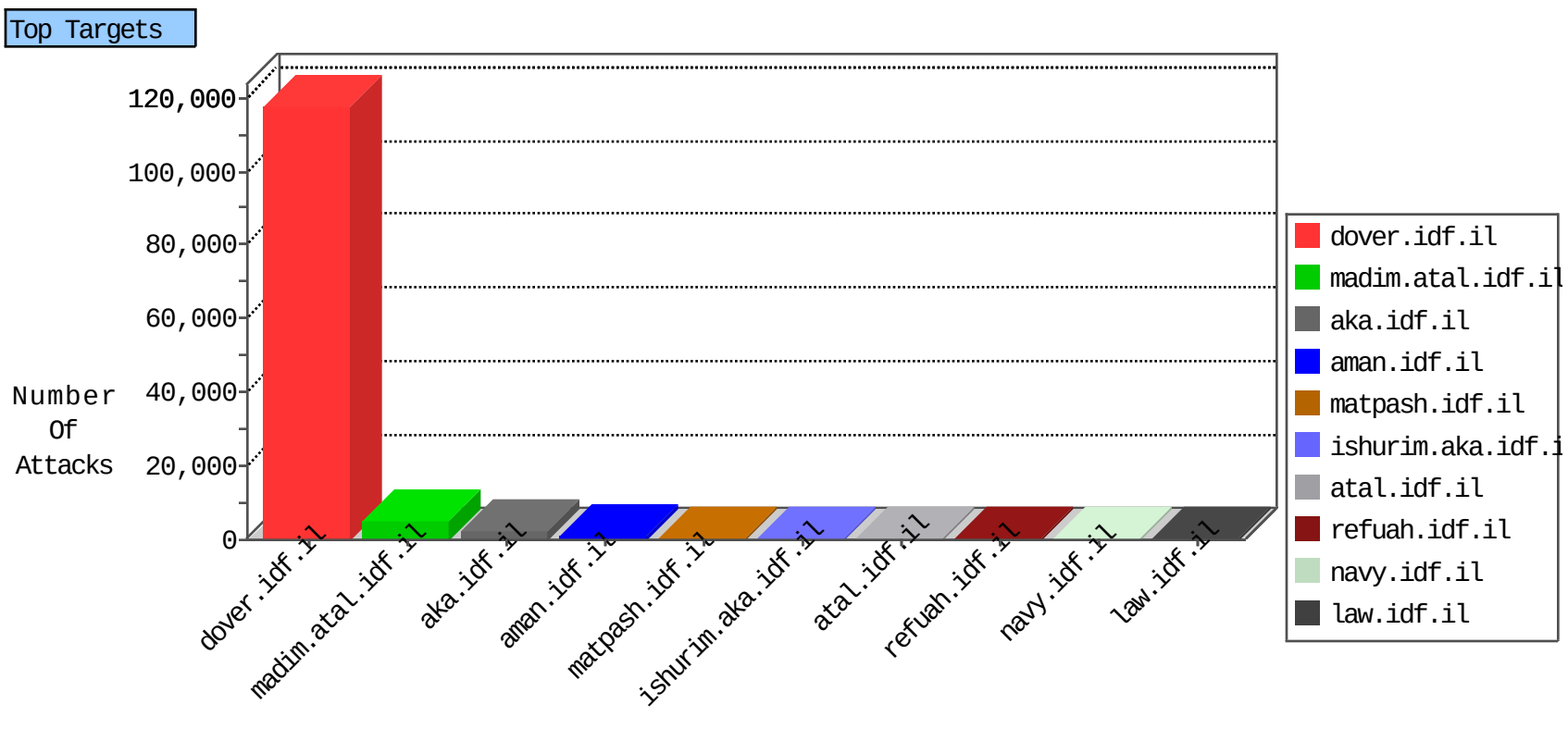
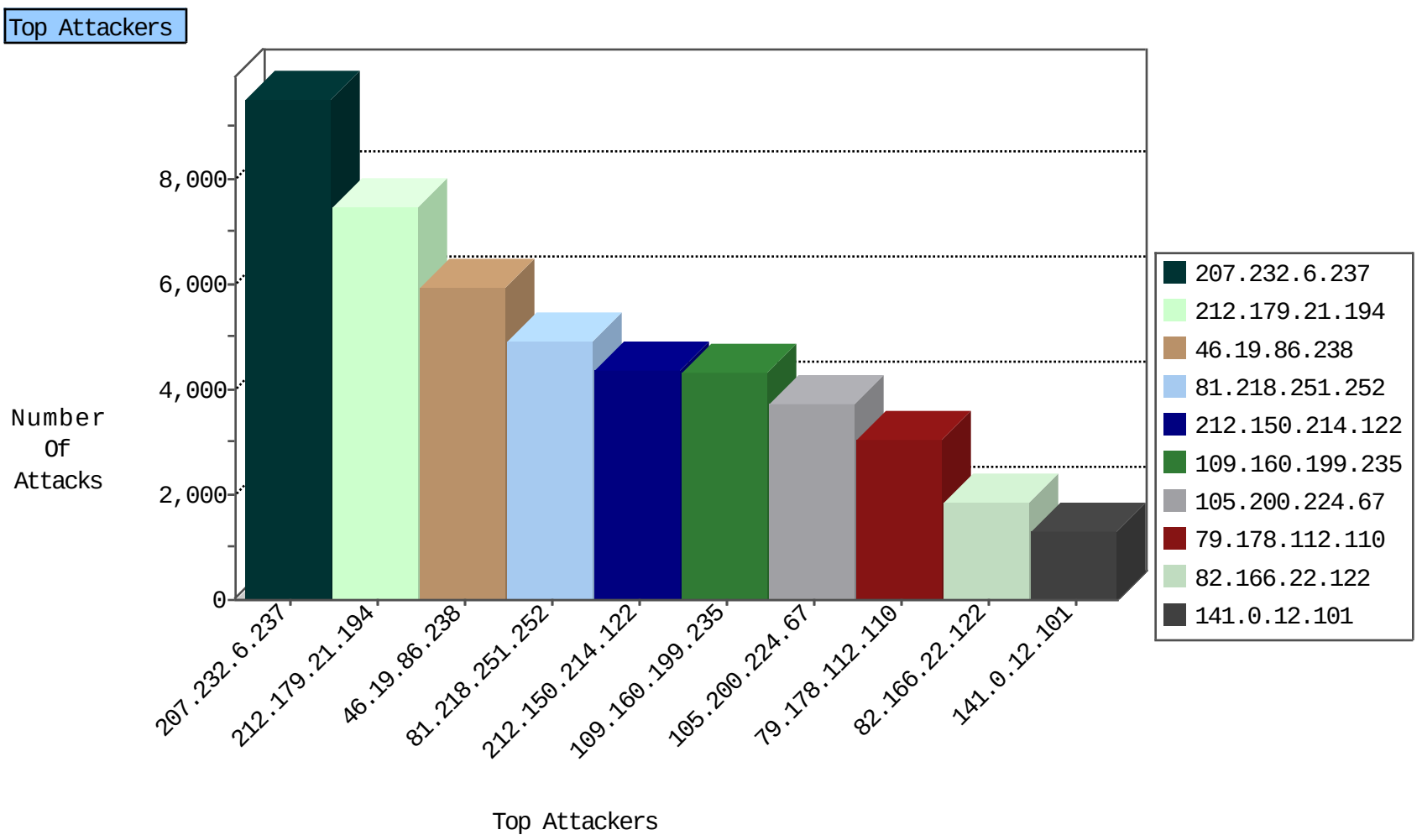
06-30-2015-00:00:02 to 07-01-2015-00:00:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



06-30-2015-00:00:02 to 07-01-2015-00:00:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.67.65	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	25442
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7123
66.249.67.59	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6135
108.59.253.71	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3619
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	2819
37.26.148.243	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2777
77.127.204.103	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	2763
46.117.187.128	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2629
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	1296
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	987
79.180.104.7	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	692
84.110.85.92	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	671
220.181.108.140	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	532
87.69.205.126	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	432
82.80.17.163	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	430
41.42.17.69	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	400
84.110.60.203	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	346
89.139.63.92	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	343
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	301
82.102.172.26	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	295
41.101.151.50	Algeria	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	263
46.19.85.11	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	246
109.64.3.210	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	226
198.52.155.201	United States	147.237.0.34	tikshuv.idf.il	HTTP-POST-Segmented-DoS	dest-reset	218
84.228.193.198	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	210
220.181.108.100	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	203
188.120.151.197	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	191
2.54.158.239	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	187
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	Web-etc/passwd-Dir-Traversal	dest-reset	184
46.116.237.240	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	182
109.64.166.132	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	159
149.88.201.6	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	158
46.117.228.77	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	158
77.125.96.85	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	155
46.117.136.6	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	154
41.101.153.69	Algeria	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	147
79.180.23.239	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	142
70.199.108.200	United States	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	142
5.29.108.90	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	139
46.121.72.85	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	138
2.54.18.241	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	138
46.246.27.211	Sweden	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	134
77.127.84.101	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
79.179.4.147	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	124
79.176.125.9	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
46.120.131.30	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
87.68.67.9	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
82.80.17.247	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	112
2.54.2.17	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
109.186.156.78	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110

06-30-2015-00:00:02 to 07-01-2015-00:00:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.127.204.103	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	281
213.139.52.15	Jordan	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	17
81.218.97.114	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
213.139.52.15	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
132.74.211.116	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
106.185.46.214	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
192.115.248.2	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
213.139.53.22	Jordan	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.182.204.225	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.120.75.136	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
46.19.85.12	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.45	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.52.155.201	United States	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.109.8.177	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
147.236.138.212	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
85.250.165.23	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
213.139.53.22	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.152	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
84.95.126.136	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
81.218.48.37	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
77.125.247.227	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
81.218.48.37	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
79.182.132.31	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
147.236.38.29	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
213.8.44.143	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
83.244.87.43	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.177.25.159	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
212.179.49.226	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
178.43.39.25	Poland	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
77.127.57.35	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
84.109.125.163	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
212.25.67.206	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
37.142.148.85	Israel	147.237.76.86	navy.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.242	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
212.199.218.50	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
197.243.86.175	Rwanda	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.176.200.112	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
94.230.86.160	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
212.25.106.78	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
5.42.238.98	Saudi Arabia	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.90	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
82.166.22.122	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
192.116.177.210	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
80.246.136.27	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.181.5.41	Israel	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	2
93.220.52.39	Germany	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
81.218.168.202	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.115	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
82.213.0.42	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
50.245.56.54	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

06-30-2015-00:00:02 to 07-01-2015-00:00:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	83
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	79
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	SQL union select - possible sql injection attempt - GET parameter	78
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	26
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	21
88.241.35.170	Turkey	147.237.77.74	law.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	12
91.215.62.8	Ukraine	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	7
88.241.35.170	Turkey	147.237.77.216	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
88.241.35.170	Turkey	147.237.77.170	maarachot.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
88.241.35.170	Turkey	147.237.77.176	matpash.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
41.42.17.69	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP JBoss JMX console access attempt	4
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	4
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Poison Null Byte	4
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	SQL Injection - Select From	4
41.42.17.69	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	3
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP cat%20 access	3
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	3
41.42.17.69	Egypt	147.237.77.216	dover.idf.il	ET WEB_SPECIFIC_APPS Possible JBoss JMX Console Beanshell Deployer WAR Upload and Deployment Exploit Attempt	3
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
43.255.188.134	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	SERVER-IIS cmd.exe access	2
61.240.144.67	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	2
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP way-board access	2
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	2
66.249.79.42	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
61.183.128.6	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	2
113.240.250.156	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.67.65	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.134	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	2
66.249.67.53	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
164.215.110.5	United States	147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	2
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	2
61.240.144.67	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	2
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP way-board.cgi access	2
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	2
61.240.144.67	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.134	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	2
41.42.17.69	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	2
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	2
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	2
43.255.188.132	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
105.200.224.67	Egypt	147.237.77.216	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	2
176.12.141.60	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.188.130	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
77.125.166.37	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
58.253.96.122	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -f -sS	1

06-30-2015-00:00:02 to 07-01-2015-00:00:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
207.232.6.237	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9537
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7419
46.19.86.238	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5949
81.218.251.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4928
212.150.214.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4372
109.160.199.235	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4335
79.178.112.110	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3032
105.200.224.67	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2484
82.166.22.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1823
141.0.12.101	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1293
77.125.166.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1196
213.204.103.36	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	920
41.101.153.69	Algeria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	901
46.19.85.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	826
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	824
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	737
37.26.147.148	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	718
46.19.85.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	653
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	626
85.65.247.25	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	614
2.54.23.55	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	602
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	597
79.182.39.238	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	584
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	565
192.116.218.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	504
109.186.0.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	495
66.249.81.212	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	492
66.249.67.53	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	476
66.249.67.65	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	462
66.249.81.218	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	447
223.225.223.240	India	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	444
66.249.67.59	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	438
212.179.230.180	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	432
197.117.116.136	Algeria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	431
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	417
66.249.81.215	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	413
190.24.146.71	Colombia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	382
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	365
212.25.102.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	360
82.145.219.46	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	358
41.101.151.50	Algeria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	352
78.89.73.52	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	344
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	321
79.177.135.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	302
67.61.58.152	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	284
194.90.229.225	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	283
213.204.127.33	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	278
66.249.67.59	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	268
46.19.85.142	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	267
70.30.66.116	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	252

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
82.102.141.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	791
176.12.149.217	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.149.217	Block	628
95.86.72.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	540
2.54.30.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	431
2.52.24.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	411
46.19.85.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	403
37.26.146.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	326
2.54.24.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	165
2.54.186.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	157
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	136
2.54.4.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	134
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	128
176.12.140.223	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.140.223	Block	120
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	113
5.29.31.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	105
2.54.157.8	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.157.8	Block	89
79.177.190.74	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.177.190.74	Block	83
176.12.148.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
149.88.43.61	United States	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	61
185.32.178.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	53
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	47
46.19.86.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	45
46.19.85.204	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.204	Block	45
176.12.141.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	42
213.151.49.189	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.151.49.189	Block	41
176.12.140.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	34
46.19.85.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	28
176.12.140.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	27
176.12.141.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	20
176.12.150.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	18
46.19.86.206	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.206	Block	17
79.177.184.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.177.184.106	Block	17
46.116.205.105	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	17
176.13.21.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
46.19.86.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
2.52.4.149	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	12
62.219.50.56	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	12
81.218.135.55	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	11
89.139.58.238	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	10
109.66.152.1	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	10
46.19.85.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
46.121.220.209	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	10
109.160.211.220	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	9
149.78.242.212	United States	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	9
178.119.119.39	Belgium	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 178.119.119.39	Block	8
200.53.156.168	Mexico	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
109.67.144.226	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.67.144.226	Block	7
109.67.144.226	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	7
84.109.205.113	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
176.13.23.82	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	6