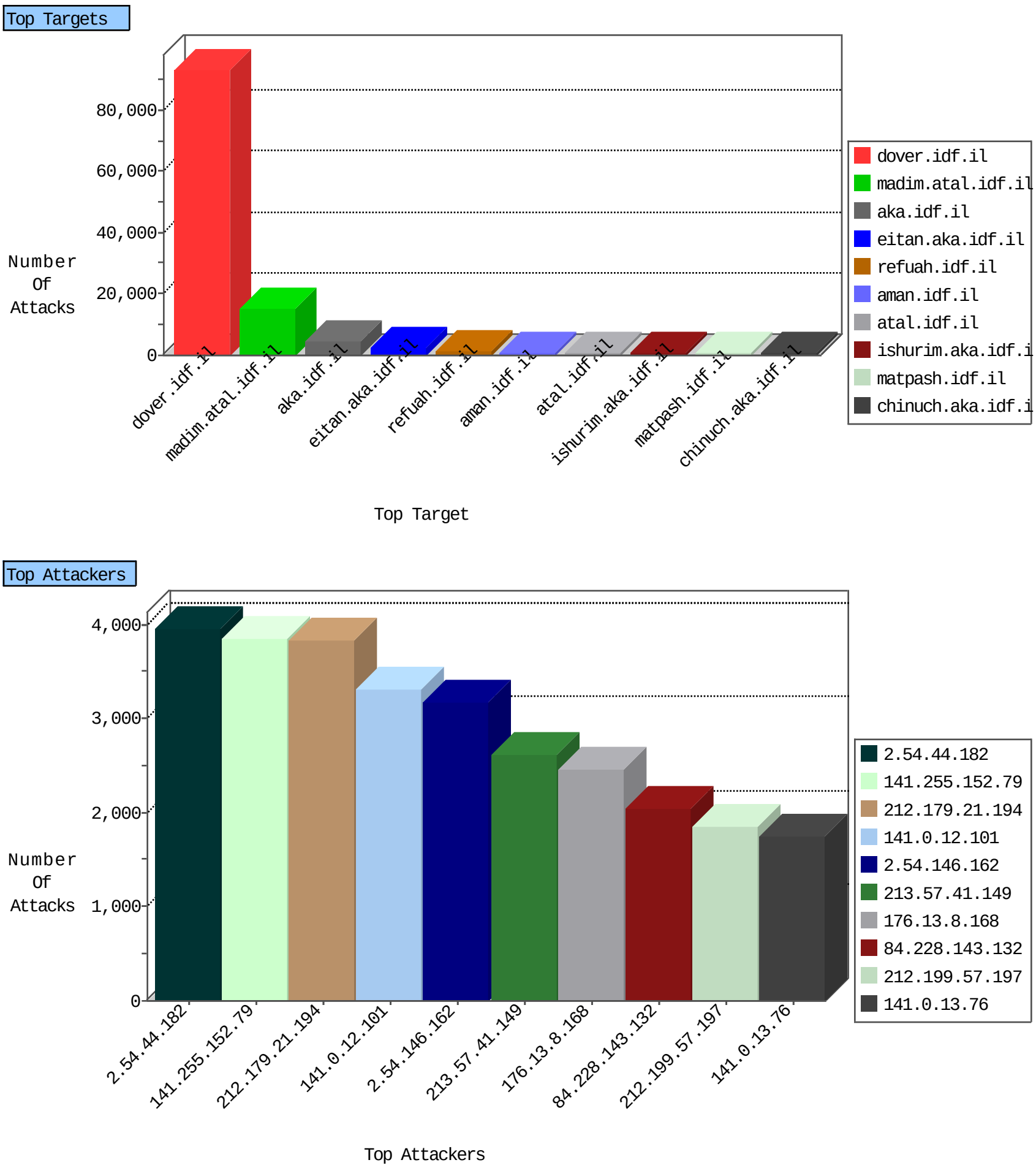
08-26-2015-00:00:09 to 08-27-2015-00:00:09

IDF Under Attack Daily Report



08-26-2015-00:00:09 to 08-27-2015-00:00:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
5.108.15.180	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	17889
64.233.172.171	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9917
54.244.22.103	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7417
64.233.172.155	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6212
66.249.69.42	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2698
141.255.152.79	Netherlands	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	1125
220.181.108.163	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	1089
84.94.173.11	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	852
79.177.149.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	744
46.120.124.175	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	593
141.0.13.76	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	387
77.126.36.39	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	336
178.77.166.124	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	335
46.116.65.10	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	268
109.186.37.200	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	258
77.126.16.189	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	225
84.108.96.204	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	219
2.52.38.9	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	210
109.64.62.211	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	203
79.176.20.166	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	194
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	188
46.116.111.16	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
46.117.73.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
109.67.173.30	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
79.177.26.239	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
192.114.2.36	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	163
93.173.239.38	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	157
93.172.171.239	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	152
84.228.161.29	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	148
213.151.47.127	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	143
176.106.227.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	143
93.173.227.254	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	142
80.179.187.146	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	141
79.177.37.10	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	140
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	130
77.127.238.175	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	124
212.25.84.200	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
79.182.137.188	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	111
188.161.195.47	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	105
109.65.107.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
31.154.91.239	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
132.70.66.11	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
77.126.62.253	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	93
79.183.122.76	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	90
46.19.85.183	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
95.86.68.4	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	87
46.19.86.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
46.120.34.43	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
213.57.231.142	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77

08-26-2015-00:00:09 to 08-27-2015-00:00:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
93.173.60.200	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	22
105.163.97.55	Kenya	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	19
62.90.220.150	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	19
77.126.36.39	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	15
192.115.21.197	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	15
46.19.85.175	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	14
41.67.117.54	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	14
104.155.193.30		147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
104.155.193.30		147.237.72.166	aka.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
104.155.193.30		147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
104.155.193.30		147.237.77.74	law.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
41.218.183.217	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	12
46.19.85.210	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	9
82.166.23.108	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	9
207.232.36.85	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
46.19.85.187	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	8
176.106.226.4	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	7
160.167.3.55		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	7
46.19.85.210	Israel	147.237.76.30	himush.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
37.19.115.4	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
212.25.80.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
109.65.107.86	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
194.8.226.84	Finland	147.237.77.74	law.idf.il	20114: HTTP: PHP Malicious Archive File Tansfer	Block	6
79.176.32.220	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
194.8.226.84	Finland	147.237.77.176	matpash.idf.il	20114: HTTP: PHP Malicious Archive File Tansfer	Block	6
212.117.135.226	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	5
213.57.229.131	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	5
84.110.7.70	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
211.59.8.170	Korea, Republic of	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
37.75.215.148	Palestinian Territory, Occupied	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
5.29.147.121	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
89.139.174.255	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.44	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
46.19.85.106	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
194.90.66.9	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
2.54.62.66	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
46.19.85.49	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
111.237.182.115	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
115.135.187.81	Malaysia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
68.192.187.225	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
123.1.192.208	Hong Kong	147.237.72.166	aka.idf.il	8479: HTTP: Suspicious HTTP Request	Block	3
217.55.241.228	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
109.65.138.114	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
212.199.146.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
109.64.49.12	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
37.75.215.148	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
46.117.17.175	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
176.127.80.75	Switzerland	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
46.19.85.113	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2

08-26-2015-00:00:09 to 08-27-2015-00:00:09

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	57
164.127.188.198	Poland	147.237.0.34	tikshuv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	9
105.158.185.67	Morocco	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	6
105.158.185.67	Morocco	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	6
105.158.185.67	Morocco	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	5
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	5
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	4
66.249.78.158	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
197.41.135.12	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP login.htm access	3
105.158.185.67	Morocco	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	3
105.158.185.67	Morocco	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	3
2.54.152.138	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
66.249.81.220	United States	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sA (2)	2
46.19.85.98	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
41.239.41.81	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	2
45.114.11.44		147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
141.255.152.79	Netherlands	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
45.114.11.44		147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
138.59.43.93	United States	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
111.51.200.118	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
79.178.191.231	Israel	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	2
199.203.59.121	Israel	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
104.155.193.30		147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	2
45.114.11.49		147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
178.252.164.247	Iran, Islamic Republic of	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
122.10.102.44	Hong Kong	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
208.80.155.216	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
151.252.81.0	Russian Federation	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
5.29.4.188	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
54.67.99.12	United States	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 2048	2
31.154.91.193	Israel	147.237.72.156	aman.idf.il	INDICATOR-SCAN ipEye SYN scan	2
54.67.99.12	United States	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -f -sS	2
45.114.11.44		147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
41.239.41.81	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP adminlogin access	2
52.16.53.214	United States	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	2
138.59.43.93	United States	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
66.249.69.42	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
197.41.135.12	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	2
45.114.11.44		147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
41.142.96.40	Morocco	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
185.5.152.52	Saudi Arabia	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
45.114.11.44		147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
122.10.102.44	Hong Kong	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
122.10.102.44	Hong Kong	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
202.71.25.29	India	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
52.28.134.251	United States	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1

08-26-2015-00:00:09 to 08-27-2015-00:00:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.54.44.182	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3964
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3518
141.0.12.101	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3312
141.255.152.79	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3202
213.57.41.149	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2613
141.0.13.76	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1732
212.179.46.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1512
31.154.167.236	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1237
54.187.55.213	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	977
212.143.40.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	939
208.109.97.62	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	812
208.109.97.62	United States	147.237.77.216	dover.idf.i	SAM rule	drop	drop	788
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	734
149.255.224.69	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	681
190.31.136.16	Argentina	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	668
85.250.101.39	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	647
8.37.227.9	Anonymous Proxy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	638
77.125.222.196	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	614
2.54.7.101	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	590
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	588
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	572
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	560
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	529
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	506
68.180.228.112	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	460
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	434
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	392
165.51.190.223		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	358
70.199.75.106	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	355
54.244.22.103	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	348
203.81.85.66	Myanmar	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	311
66.249.69.26	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	308
66.249.69.42	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	307
66.249.69.34	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	292
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	291
70.39.184.158	Satellite Provider	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	265
2.52.0.64	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	264
92.241.34.180	Jordan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	262
107.77.70.119	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	258
82.145.208.129	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	258
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	239
2.54.44.135	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	238
81.246.118.4	Belgium	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	234
79.221.123.245	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	230
157.55.39.124	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	227
95.86.123.40	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	212
213.177.14.146	Romania	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	211
62.219.111.242	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	209
80.241.255.91	Georgia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	196
31.25.138.34	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	195

08-26-2015-00:00:09 to 08-27-2015-00:00:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.146.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3179
176.13.8.168	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.8.168	Block	2465
84.228.143.132	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	2040
212.199.57.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1820
176.13.10.48	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.10.48	Block	1492
2.52.149.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1006
2.54.191.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	842
37.26.148.187	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.148.187	Block	821
176.12.143.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	756
2.54.139.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	630
46.19.85.74	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.74	Block	588
2.54.164.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	400
2.52.22.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	228
109.65.2.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	210
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.34	Block	205
176.12.136.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	178
84.108.146.208	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	162
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.42	Block	135
80.246.136.182	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.182	Block	110
197.41.135.12	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.41.135.12	Block	105
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	95
62.90.5.214	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 62.90.5.214	Block	90
79.177.37.10	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 79.177.37.10	Block	80
212.150.66.161	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.150.66.161	Block	75
46.120.84.148	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.84.148	Block	67
85.65.4.85	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 85.65.4.85	Block	65
136.243.92.96	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 136.243.92.96	Block	60
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	60
197.41.135.12	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	60
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	54
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	52
37.26.147.231	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.231	Block	50
41.239.41.81	Egypt	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	50
197.41.135.12	Egypt	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	45
84.108.48.42	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	42
66.249.64.154	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	42
41.239.41.81	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.239.41.81	Block	40
79.178.56.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	36
109.64.131.48	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.64.131.48	Block	36
198.204.249.34	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 198.204.249.34	Block	36
84.108.48.42	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.108.48.42	Block	36
176.228.214.208	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	35
79.180.213.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	35
109.64.131.48	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	30
41.239.41.81	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	30
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	30
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	30
66.249.78.128	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
176.12.144.239	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	30
109.64.131.48	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	30

08-26-2015-00:00:09 to 08-27-2015-00:00:09