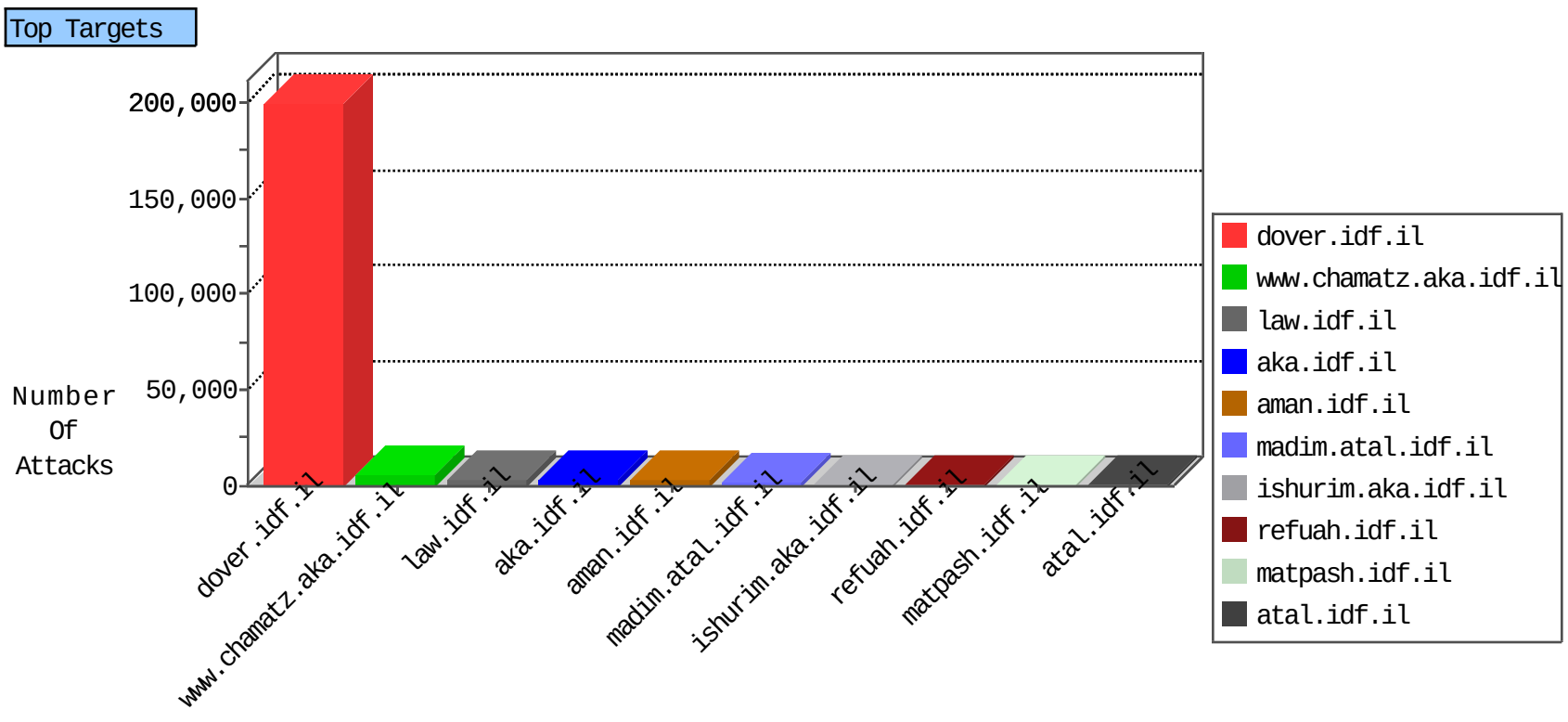
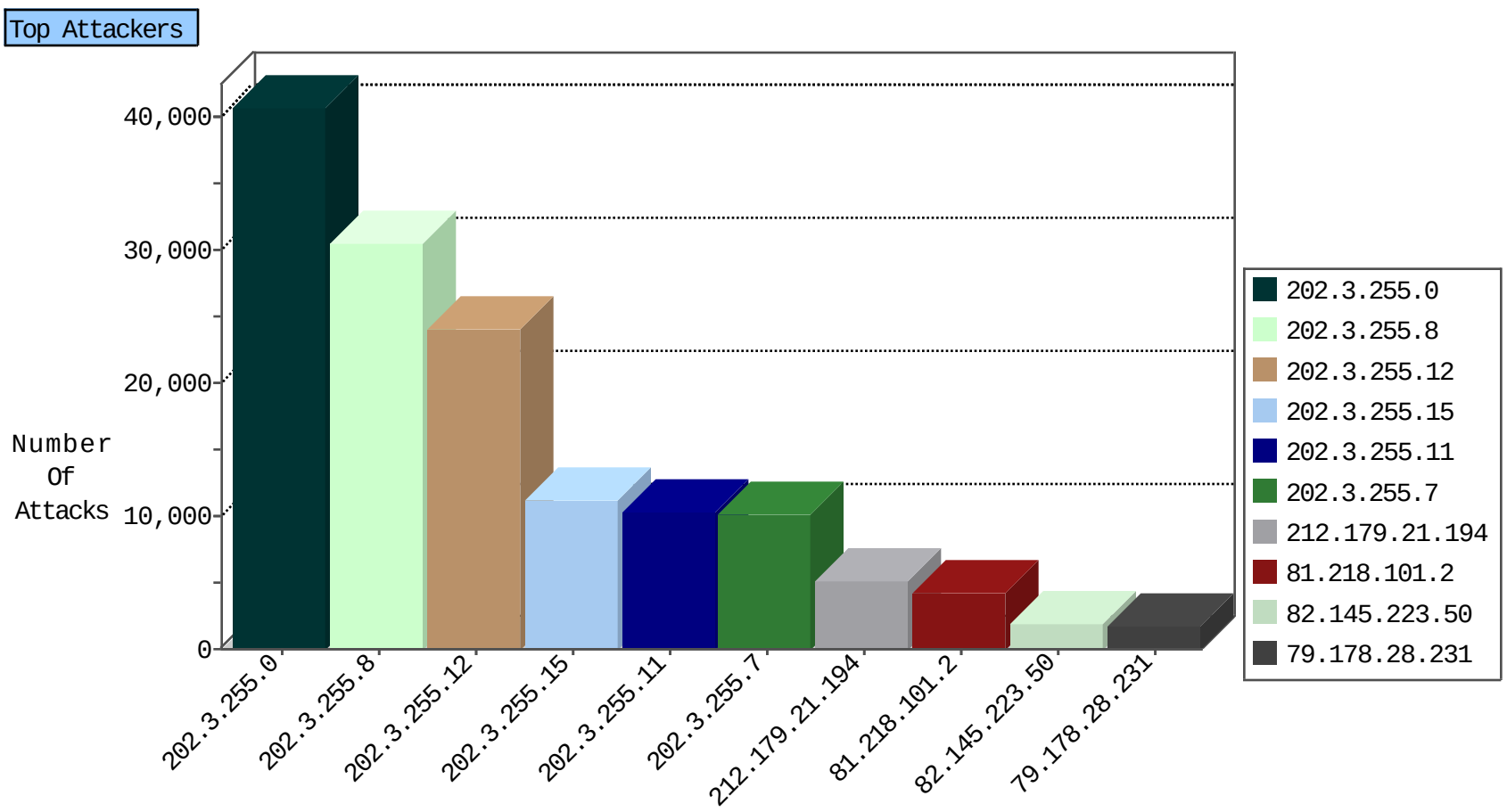
07-30-2015-00:00:09 to 07-31-2015-00:00:09

IDF Under Attack Daily Report



Top Target



Top Attackers

07-30-2015-00:00:09 to 07-31-2015-00:00:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.93.164	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	312709
108.215.57.66	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12898
66.249.65.92	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8940
38.111.147.88	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7511
184.151.111.237	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3920
77.75.77.200	Czech Republic	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2287
79.182.212.191	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	1386
82.145.223.50	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1360
167.114.156.198	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1220
89.138.73.107	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	718
204.93.154.201	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	708
213.57.105.93	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	673
213.57.186.253	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	644
207.46.13.136	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	532
109.66.35.98	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	529
93.173.159.214	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	449
77.125.82.54	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	348
79.180.108.4	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	344
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	316
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	284
109.186.76.199	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	284
79.178.1.86	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	262
87.68.159.241	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	259
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	257
85.65.5.111	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	252
46.117.140.191	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	247
10.0.0.15		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	234
197.251.241.1	Ghana	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	221
93.172.72.87	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	218
79.176.111.181	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	216
84.109.193.81	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	213
37.142.97.213	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	210
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	210
87.69.54.71	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	198
84.228.84.70	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	184
109.186.100.186	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	182
109.186.175.71	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
77.126.10.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
192.114.91.215	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	168
31.168.72.170	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
79.181.53.172	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
79.176.43.150	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	156
79.182.97.29	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	155
79.176.183.229	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	154
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	148
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	133
46.120.137.166	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
212.117.151.70	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	131
79.181.100.251	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	126
79.182.50.148	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123

07-30-2015-00:00:09 to 07-31-2015-00:00:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
112.111.188.255	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	23
213.139.53.37	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	16
85.65.5.111	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	16
213.8.245.50	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	15
213.8.245.58	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	15
46.117.140.191	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
84.109.193.81	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
79.176.43.150	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
84.228.84.70	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
85.64.107.224	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
93.172.186.228	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
37.26.148.192	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
62.90.194.104	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
109.66.142.149	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
223.176.6.200	India	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.168	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
213.57.249.158	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
2.54.183.66	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.109.96.31	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
2.52.61.82	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.29	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
109.66.142.149	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
79.178.117.209	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
89.248.172.169	Netherlands	147.237.77.74	law.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	4
89.185.247.72	Czech Republic	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
115.146.123.160	Vietnam	147.237.72.167	ishurim.aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
89.248.172.169	Netherlands	147.237.77.234	halag.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	4
89.248.172.169	Netherlands	147.237.77.170	maarachot.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	4
89.139.54.223	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
89.248.172.169	Netherlands	147.237.72.156	aman.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	4
85.64.42.223	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
89.248.172.169	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	4
89.185.247.72	Czech Republic	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
5.29.143.51	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
192.116.94.74	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
79.182.97.29	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.66.129.154	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
62.219.160.95	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
93.172.202.185	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.120.195.186	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.183.9.154	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
58.10.150.174	Thailand	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
89.138.40.220	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.111.140.141	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.26	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
176.67.111.250	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.250.67.153	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.228.123.85	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
212.179.21.194	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

07-30-2015-00:00:09 to 07-31-2015-00:00:09

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
202.3.255.0	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	37226
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	27909
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	22080
202.3.255.15	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	10186
202.3.255.11	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	9360
202.3.255.7	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	9282
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	109
2.52.181.137	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	15
37.237.106.223	Iraq	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	12
37.237.106.223	Iraq	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	9
37.237.106.223	Iraq	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	9
37.237.106.223	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	9
37.237.106.223	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	9
37.237.106.223	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	9
37.237.106.223	Iraq	147.237.77.216	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	9
37.237.106.223	Iraq	147.237.77.216	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	9
37.237.106.223	Iraq	147.237.77.216	dover.idf.il	SERVER-IIS cmd.exe access	9
37.237.106.223	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	9
37.237.106.223	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	9
37.237.106.223	Iraq	147.237.77.216	dover.idf.il	SQL Injection - Select From	9
27.75.101.97	Vietnam	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	8
37.237.106.212	Iraq	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	8
27.75.101.97	Vietnam	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	8
37.237.106.212	Iraq	147.237.77.216	dover.idf.il	SQL Injection - Select From	7
37.237.106.223	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt	7
37.237.104.105	Iraq	147.237.77.216	dover.idf.il	SQL Injection - Select From	6
37.237.104.109	Iraq	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	6
109.65.75.213	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
37.237.106.212	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	5
37.237.106.212	Iraq	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	5
37.237.106.177	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	4
37.237.104.109	Iraq	147.237.77.216	dover.idf.il	SQL Injection - Select From	4
37.237.106.212	Iraq	147.237.77.216	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	4
37.237.106.177	Iraq	147.237.77.216	dover.idf.il	SQL Injection - Select From	4
37.237.106.212	Iraq	147.237.77.216	dover.idf.il	SERVER-IIS cmd.exe access	4
41.105.118.144	Algeria	147.237.77.216	dover.idf.il	ET SCAN Netsparker Default User-Agent	4
37.237.106.212	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	4
37.237.106.212	Iraq	147.237.77.216	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	4
37.237.106.212	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt	4
37.237.106.212	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	4
37.237.106.212	Iraq	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	4
45.114.11.47		147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	4
37.237.106.212	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	4
37.237.106.177	Iraq	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	4
37.237.104.109	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	4
37.237.104.228	Iraq	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	4
37.237.106.212	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	4
37.237.104.109	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	3
37.237.106.177	Iraq	147.237.77.216	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	3
37.237.104.228	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	3

07-30-2015-00:00:09 to 07-31-2015-00:00:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4899
81.218.101.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4299
202.3.255.0	French Polynesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3603
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2703
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2052
82.145.223.50	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1819
79.178.28.231	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1721
213.8.242.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1461
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1438
202.3.255.15	French Polynesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	957
38.111.147.88	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	929
202.3.255.7	French Polynesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	901
202.3.255.11	French Polynesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	900
84.108.48.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	887
120.210.180.144	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	756
89.139.184.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	688
46.19.85.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	658
188.165.15.94	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	574
66.249.65.92	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	566
66.249.65.89	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	544
54.187.55.213	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	542
66.249.65.95	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	524
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	508
79.183.18.175	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	505
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	484
2.54.174.67	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	482
46.19.86.189	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	481
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	456
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	445
79.176.155.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	419
31.168.194.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	409
109.186.76.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	390
79.179.102.141	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	332
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	315
5.102.254.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	314
109.65.25.204	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	306
66.85.148.53	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	279
94.249.211.243	Germany	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	276
94.249.246.192	Germany	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	267
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	261
213.204.103.36	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	251
36.79.116.222	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	239
157.55.39.203	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	234
66.249.93.164	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	233
68.180.228.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	233
94.249.211.222	Germany	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	232
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	225
5.255.253.33	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	219
93.127.140.253	Germany	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	212
2.54.27.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	212

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
80.246.136.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	736
2.54.48.230	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.48.230	Block	436
66.249.65.89	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.89	Block	236
66.249.65.95	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.95	Block	228
66.249.65.92	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.92	Block	220
2.54.181.207	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.181.207	Block	192
188.143.232.34	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.34	Block	152
2.54.168.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	116
176.13.10.95	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.10.95	Block	112
80.246.136.116	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.116	Block	96
176.12.148.171	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.148.171	Block	92
176.13.15.132	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.15.132	Block	54
188.165.15.94	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.94	Block	40
193.201.224.126	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 193.201.224.126	Block	36
115.78.235.170	Vietnam	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	36
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	32
79.179.134.222	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 79.179.134.222	Block	30
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
46.116.131.3	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	24
212.143.173.198	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 212.143.173.198	Block	22
114.230.128.97	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 114.230.128.97	Block	20
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	18
87.68.46.120	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	16
66.249.65.89	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	16
66.249.65.92	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	16
2.54.185.57	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	16
66.249.65.95	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	12
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	12
80.246.137.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
37.26.146.179	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
79.180.28.216	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	12
188.165.15.27	France	147.237.76.30	himush.idf.il	Unknown Parameter l in www.chimush.atal.idf.il/templates/sendtofriend/sendtofriend.aspx	None	12
46.119.124.209	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17155-en/	Block	12
176.228.40.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
80.246.137.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
46.19.85.152	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	10
212.97.132.130	Denmark	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.97.132.130	Block	10
79.176.176.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	10
192.114.163.66	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 192.114.163.66	Block	10
46.118.117.215	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17155-en/	Block	10
212.116.182.92	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 212.116.182.92	Block	10
109.65.202.156	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
46.19.85.144	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
91.200.12.9	Ukraine	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 91.200.12.9	Block	8
109.65.148.147	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
46.19.86.100	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
213.57.152.163	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
91.200.12.9	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	8
91.200.12.9	Ukraine	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 91.200.12.9	Block	8
37.237.106.212	Iraq	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.237.106.212	Block	8

07-30-2015-00:00:09 to 07-31-2015-00:00:09