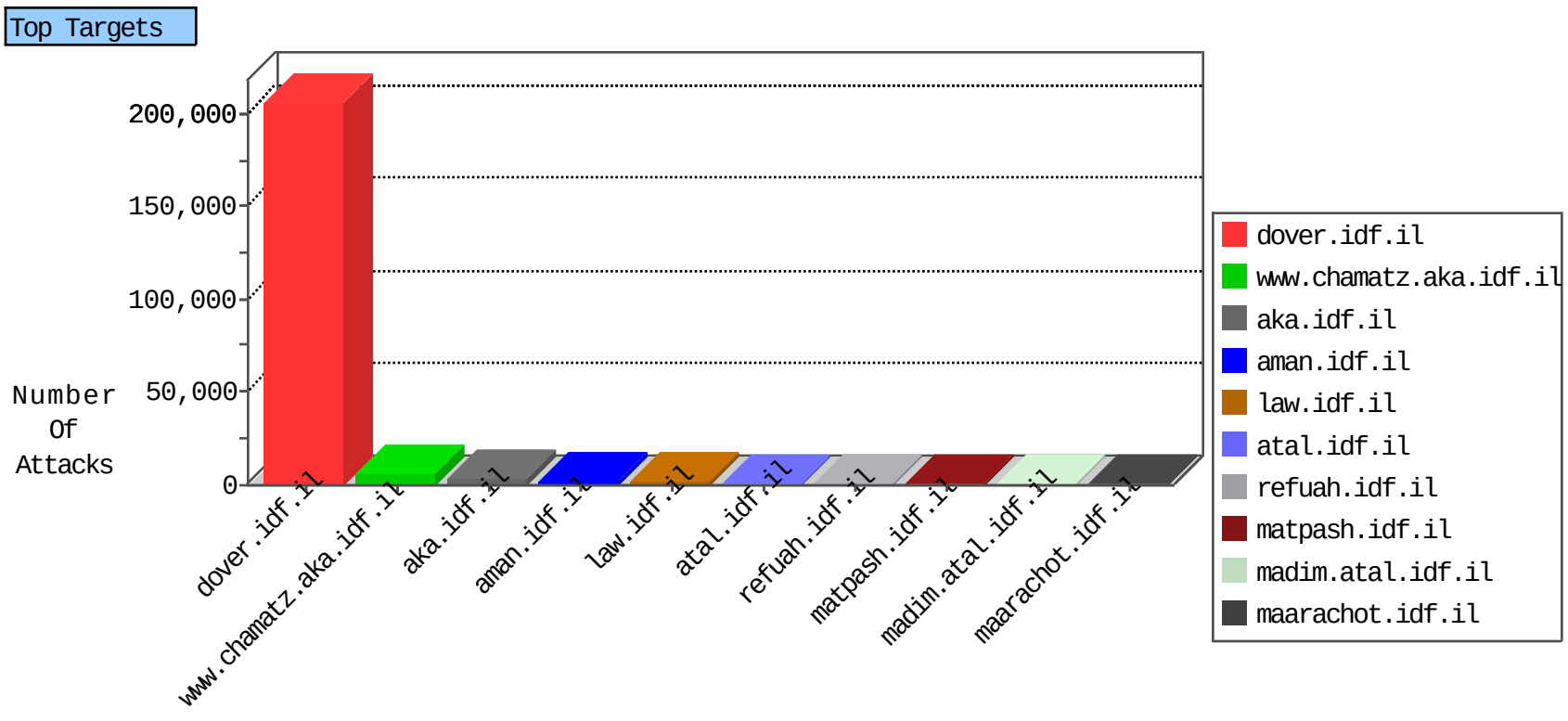
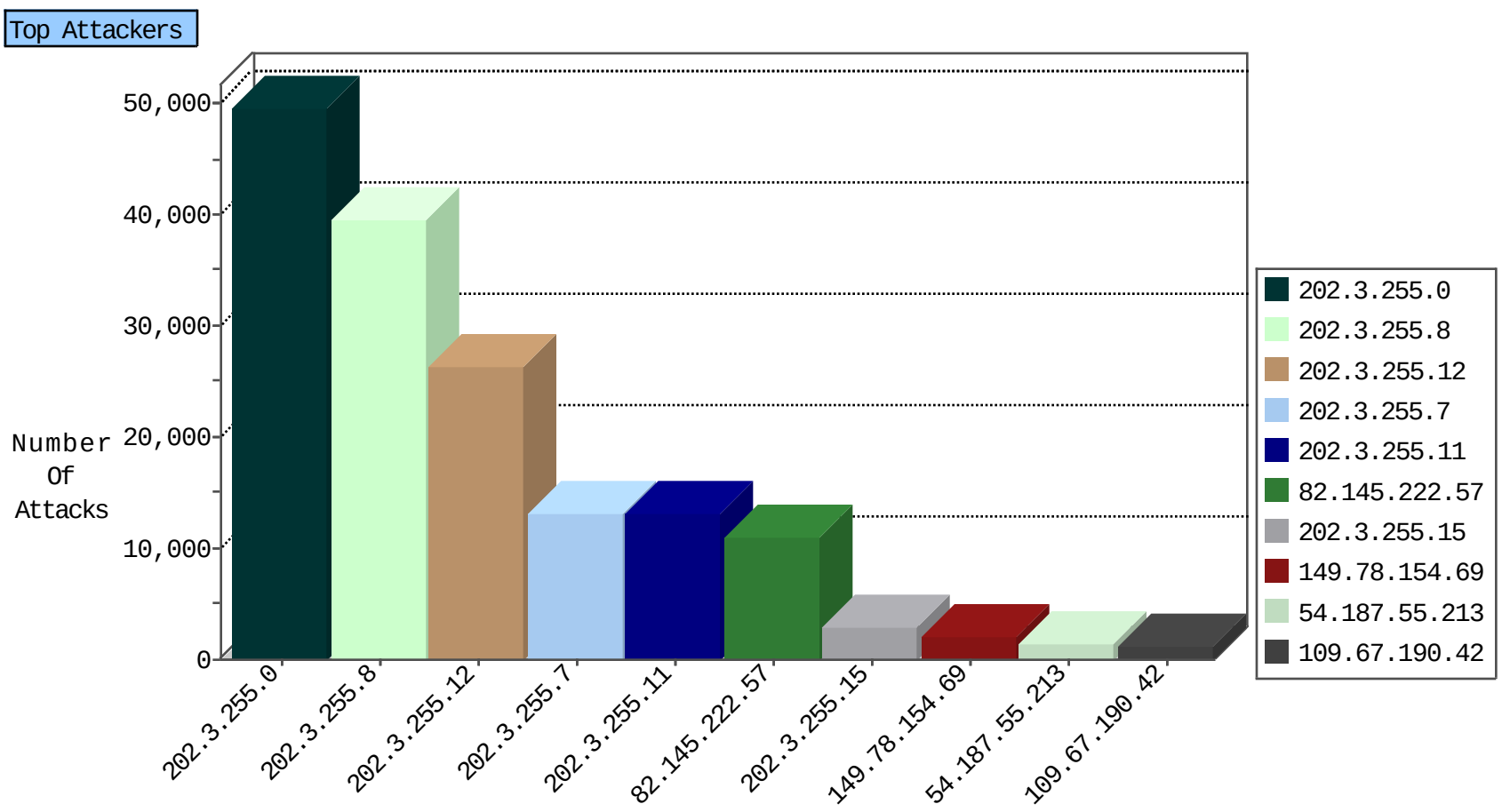
07-31-2015-00:00:05 to 08-01-2015-00:00:05

IDF Under Attack Daily Report



Top Target



Top Attackers

07-31-2015-00:00:05 to 08-01-2015-00:00:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.65.89	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	41816
66.249.93.164	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	30596
202.3.255.11	French Polynesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	22269
202.3.255.0	French Polynesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	21661
66.249.65.92	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	18736
66.249.93.168	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15911
82.145.222.57	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15801
46.107.102.131	Hungary	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15615
66.249.65.95	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15372
82.211.18.50	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15336
62.210.97.48	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	13512
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12915
188.161.194.251	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12534
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11084
54.187.55.213	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8753
66.249.64.156	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	8368
66.249.67.73	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	7031
66.249.93.243	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	5047
54.72.73.168	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3426
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	3416
66.249.67.81	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3372
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	3241
186.91.159.166	Venezuela	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3164
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	2749
193.24.32.44	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2588
2.69.42.109	Sweden	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1979
103.27.171.49	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1313
79.177.63.158	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	864
79.181.174.10	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	729
84.111.64.178	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	602
5.175.200.44	Germany	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	588
206.112.75.195	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	533
79.180.99.81	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	356
87.68.31.206	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	348
37.237.160.26	Iraq	147.237.77.216	dover.idf.il	HTTP-MISC-Havij-User-Agent	dest-reset	326
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	320
46.116.116.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	266
87.69.10.88	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	231
82.145.209.17	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	204
5.22.129.212	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
149.88.97.81	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	200
79.183.113.62	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	183
79.177.49.142	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
87.68.146.128	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
79.181.150.61	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
84.228.61.39	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
79.182.188.208	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
79.182.23.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
109.65.81.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
46.117.105.169	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166

07-31-2015-00:00:05 to 08-01-2015-00:00:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.177.63.158	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	53
112.111.188.255	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	13
211.149.201.209	China	147.237.76.31	nakchal.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
211.149.201.209	China	147.237.76.86	navy.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
211.149.201.209	China	147.237.76.147	chinuch.aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
211.149.201.209	China	147.237.76.30	himush.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
211.149.201.209	China	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	10
106.185.39.169	Japan	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	7
213.139.52.53	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
85.250.204.13	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
5.102.254.239	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
89.138.212.29	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
91.121.196.94	France	147.237.77.74	law.idf.il	19863: HTTP: WordPress Revslider/Showbiz PHP File Upload	Block	4
83.143.81.94	Norway	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
93.173.41.65	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
79.177.111.200	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
83.143.81.94	Norway	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
89.185.247.72	Czech Republic	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
46.19.85.245	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
209.213.104.25	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
66.135.63.82	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
74.113.112.100	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
89.185.247.72	Czech Republic	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
46.117.182.72	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.182.103.227	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
93.92.56.189	Hungary	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.177.55.68	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
222.84.5.244	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	3
109.65.127.144	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
91.121.196.94	France	147.237.77.216	dover.idf.il	19863: HTTP: WordPress Revslider/Showbiz PHP File Upload	Block	3
154.20.209.41	Canada	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.26.147.182	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	3
70.44.143.242	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
5.29.39.144	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
66.135.63.82	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3
114.230.128.97	China	147.237.77.170	maarachot.idf.il	0854: HTTP: upload* Access	Block	2
46.19.85.157	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
77.126.14.174	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
87.68.68.170	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
109.160.254.156	Israel	147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	2
130.123.96.22	New Zealand	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
103.242.217.50	Bangladesh	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.65.31.67	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
89.138.91.224	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.202	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
103.247.50.178	Sri Lanka	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
213.6.5.98	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
77.125.86.61	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
82.102.141.251	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.108	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

07-31-2015-00:00:05 to 08-01-2015-00:00:05

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	46229
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	36755
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	24498
202.3.255.7	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	12314
202.3.255.11	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	12243
202.3.255.15	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	2624
66.249.93.168	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	272
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	137
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	SQL Injection - Select From	63
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	59
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	57
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	55
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	54
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	54
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	54
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	54
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	54
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	54
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	54
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	SERVER-IIS cmd.exe access	54
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP TRACE attempt	41
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	34
66.249.67.67	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	8
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	6
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in URI	5
66.249.65.92	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
196.206.88.192	Morocco	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	4
218.65.30.107	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	3
61.240.144.66	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	3
61.183.128.6	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	3
89.248.168.128	Netherlands	147.237.8.14	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
45.114.11.49		147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	3
66.249.78.172	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
218.65.30.107	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	3
221.203.3.117	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	3
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	3
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	3
197.32.58.224	Egypt	147.237.77.216	dover.idf.il	SQL union select - possible sql injection attempt - GET parameter	3
66.249.78.165	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
66.249.67.87	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
45.114.11.48		147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
199.101.186.226	United States	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	2
221.203.3.117	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
109.65.117.229	Israel	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sA (2)	2
177.71.92.175		147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
45.114.11.48		147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2

07-31-2015-00:00:05 to 08-01-2015-00:00:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.145.222.57	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11010
202.3.255.0	French Polynesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3392
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2698
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1995
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1800
54.187.55.213	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1288
109.67.190.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1251
31.44.129.80	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1234
149.255.213.156	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	995
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
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	710
66.249.65.89	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	582
66.249.65.92	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	528
66.249.65.95	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	510
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	499
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	492
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	484
80.215.229.8	France	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	478
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	476
79.180.128.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	476
92.62.170.228	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	380
164.97.245.84	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	374
105.90.214.123	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	372
109.186.76.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	360
132.76.50.5	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	355
95.86.99.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	349
109.65.53.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	341
94.249.247.128	Germany	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	297
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	296
176.193.98.233	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	275
2.54.63.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	268
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	261
95.221.221.68	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	259
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	256
157.55.39.203	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	250
188.165.15.94	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	243
94.153.230.50	Ukraine	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	219
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	218
94.249.247.209	Germany	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	216
54.244.22.103	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	211
176.223.82.91	Germany	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	207
82.211.18.136	Germany	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	204
176.223.84.116	Germany	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	203
176.223.85.205	Germany	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	197
54.244.22.103	United States	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	196
68.180.228.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	192
202.3.255.15	French Polynesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	191
176.223.85.154	Germany	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	188
155.254.126.154		147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	185

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.65.89	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.89	Block	390
46.19.86.204	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.204	Block	384
66.249.65.92	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.92	Block	348
66.249.65.95	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.95	Block	342
109.160.173.100	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.160.173.100	Block	186
114.230.128.97	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 114.230.128.97	Block	40
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	38
188.143.232.43	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.43	Block	26
198.204.245.202	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 198.204.245.202	Block	24
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	20
183.79.221.110	Japan	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 183.79.221.110	Block	18
199.16.156.126	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.16.156.126	Block	16
199.16.156.125	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.16.156.125	Block	14
188.165.15.94	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.94	Block	14
85.64.178.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyu/miyun/miyunselectque	Block	14
68.180.228.100	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1073-he/nakhal.aspx	Block	12
77.126.233.39	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
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
77.125.3.12	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
83.247.7.29	Netherlands	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 83.247.7.29	Block	10
2.52.14.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
37.237.160.67	Iraq	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.237.160.67	Block	10
84.108.86.35	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	10
31.168.101.163	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/3/	Block	10
89.139.49.65	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	10
176.13.10.132	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
109.160.233.131	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	8
92.253.59.214	Jordan	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 92.253.59.214	Block	8
46.120.230.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	8
66.249.65.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	8
66.249.65.83	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	8
82.166.6.6	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/xmlrpc.php	Block	8
46.116.47.165	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	8
109.67.141.89	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/resource/userfollowresource/create/	Block	8
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	8
31.154.92.108	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	8
37.142.64.120	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	8
46.121.76.57	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
89.139.61.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
2.54.21.62	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1557	Block	8
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	8
82.166.6.6	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed PHP Attempt	Block	8
77.126.36.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/tzevetavirquestionaire.aspx	Block	6
79.183.51.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
85.64.128.177	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	6
176.13.15.111	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	6
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	6
176.13.2.197	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.2.197	None	6
109.65.205.187	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	6
46.121.60.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6