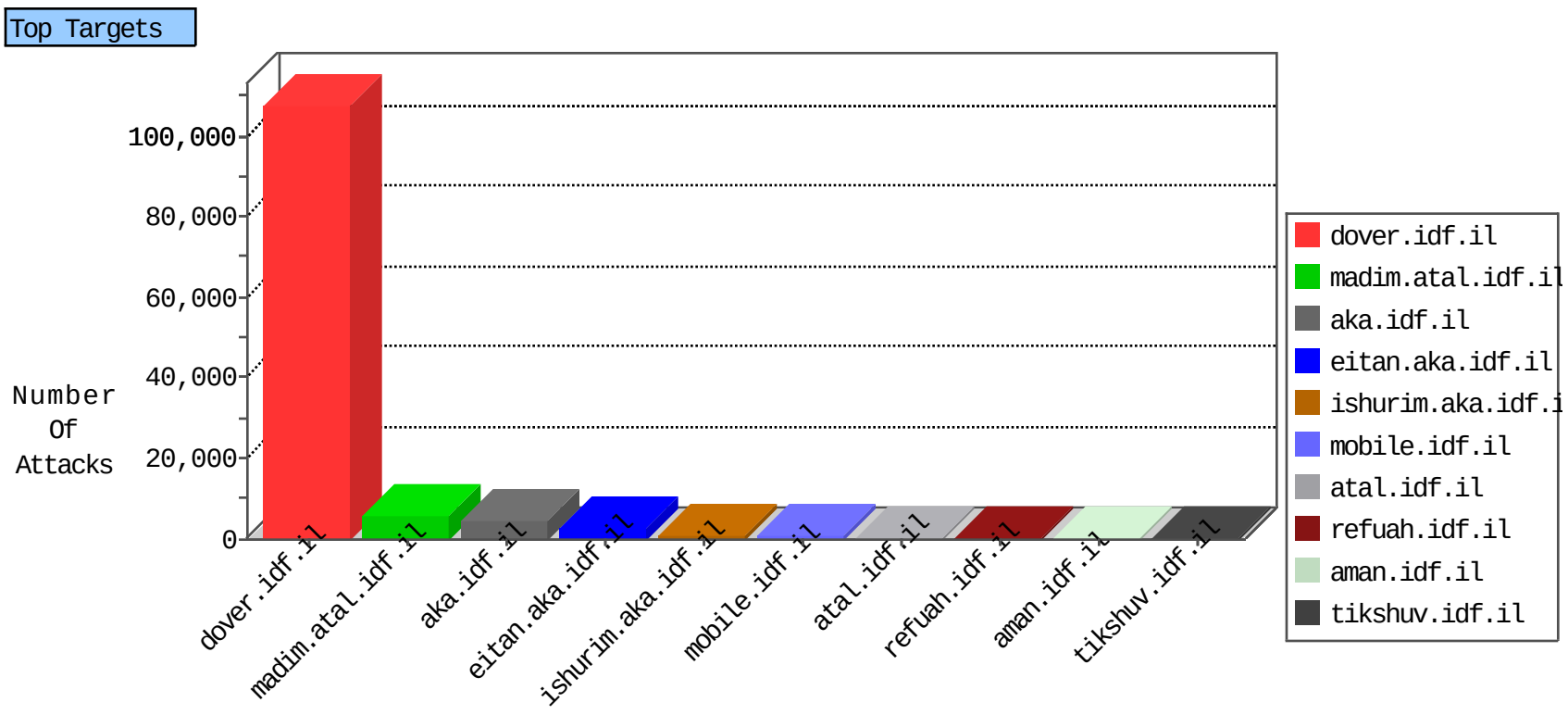
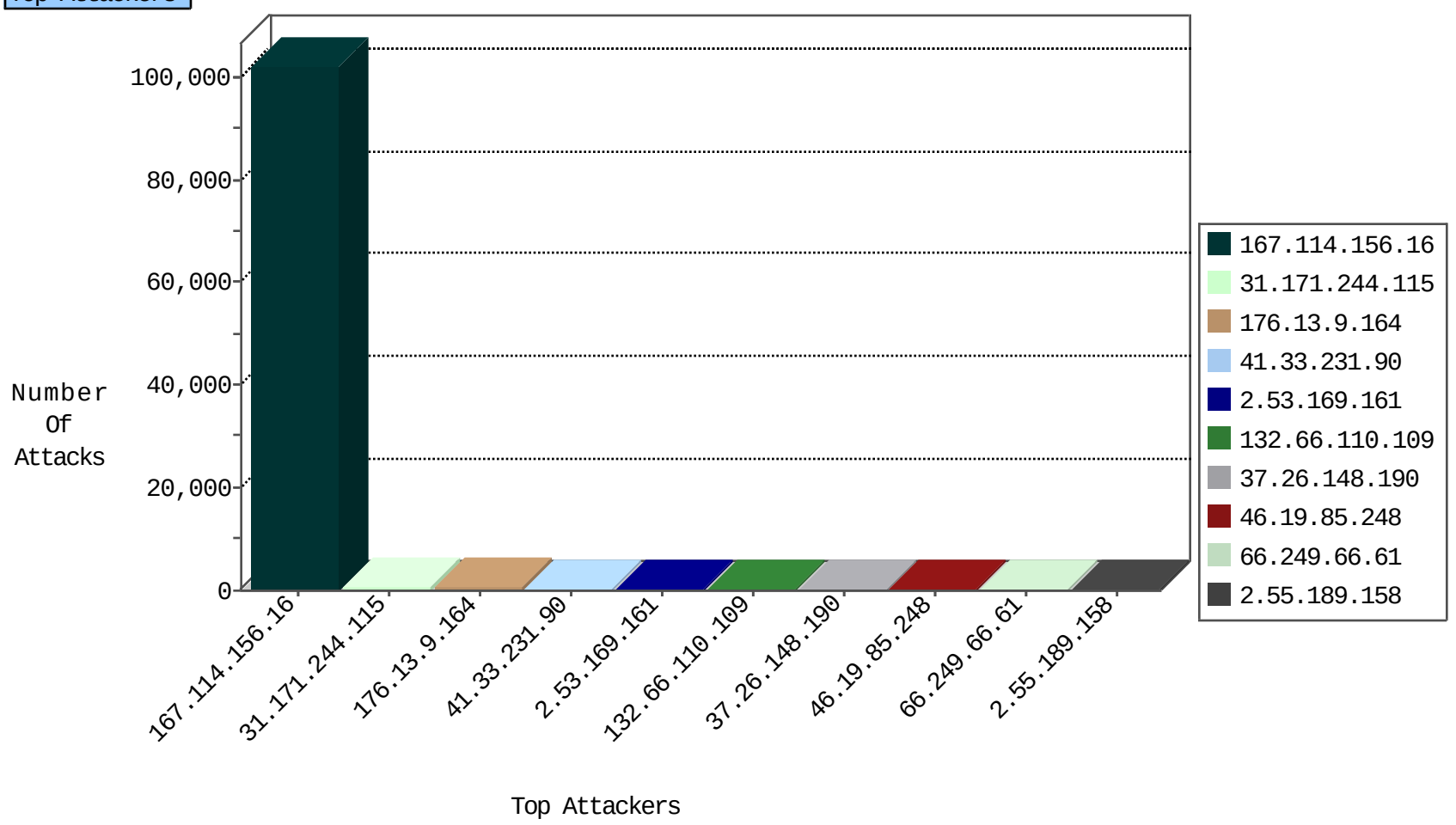
04-18-2016 to 04-19-2016

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-18-2016 to 04-19-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	101812
193.106.206.10	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5883
79.182.174.196	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2613
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	658
79.180.115.194	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	48
134.191.232.71	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	47
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	45
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	30
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	17
94.159.152.117	Israel	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	16
79.180.115.194	Israel	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	15
109.65.172.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	11
92.82.87.8	Romania	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	11
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	10
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
41.239.7.110	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
212.199.182.150	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
203.254.51.16	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
194.165.134.84	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
79.177.128.141	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
109.64.12.74	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.177.128.141	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.181.20.6	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.176.53.196	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
82.145.211.4	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
46.117.62.14	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.53.30.151	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
37.46.39.193	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
120.132.50.135	China	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	4
123.59.59.52	China	147.237.72.166	aka.idf.il	block-sp-traf1	forward	4
82.145.208.47	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
123.59.59.52	China	147.237.77.74	law.idf.il	block-sp-traf1	forward	4
120.132.50.135	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	4
104.148.71.133	United States	147.237.8.14	e.orchot.idf.il	JLM_Purple_Con_Limit_Http	drop	3
82.102.135.34	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
31.168.14.82	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.56.245	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
31.168.137.34	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
74.91.23.107	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	3
82.145.209.40	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3
80.82.78.38	Netherlands	147.237.77.233	atal.idf.il	block-sp-traf1	forward	2
202.112.51.96	China	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	2
107.150.32.59	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
202.112.51.96	China	147.237.72.156	aman.idf.il	block-sp-traf1	forward	2
69.30.202.228	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
204.12.196.237	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
74.91.20.197	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	2
185.5.30.59	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
69.30.198.147	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	2

04-18-2016 to 04-19-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.103	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	25
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	23
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	19
149.88.47.121	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
212.199.57.202	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
213.57.53.246	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
212.83.177.193	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	5
69.197.177.50	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	4
213.8.145.99	Israel	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
66.76.174.2	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
69.197.177.50	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
192.187.101.234	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
185.103.252.98	Russian Federation	147.237.76.86	navy.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	3
185.103.252.98	Russian Federation	147.237.77.234	halag.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	3
94.22.47.242	Finland	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	3
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
94.22.47.242	Finland	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.198.242	United States	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	2
192.187.101.234	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
62.210.148.246	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.61.21	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.198.202	United States	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	2
94.22.47.242	Finland	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.211.2	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.198.202	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
69.197.177.50	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
93.173.55.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.30.198.202	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
69.197.177.50	United States	147.237.76.147	chinuch.aka.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.198.202	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.197.177.50	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.66.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
185.103.252.98	Russian Federation	147.237.72.167	ishurim.aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
197.45.65.198	Egypt	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
198.20.69.74	United States	147.237.76.201	e.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
151.80.31.160	France	147.237.0.34	tikshuv.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.182	France	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
40.77.167.50	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-18-2016 to 04-19-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.88.81	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	104
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	62
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	45
93.89.19.29	147.237.0.34	Turkey	tikshuv.idf.il	SQL Injection - Select From	25
66.249.64.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	24
66.76.174.2	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	12
213.8.145.99	147.237.77.233	Israel	atal.idf.il	SQL Injection - Select From	12
193.200.80.26	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	10
213.8.145.99	147.237.72.166	Israel	aka.idf.il	SQL Injection - Select From	9
177.185.192.77	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	8
193.200.80.26	147.237.77.74	United Kingdom	law.idf.il	ET WEB_SERVER SQLi - SELECT and sysobject	7
93.89.19.29	147.237.0.34	Turkey	tikshuv.idf.il	ET WEB_SERVER SQLi - SELECT and sysobject	7
193.200.80.26	147.237.77.74	United Kingdom	law.idf.il	ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns	7
93.89.19.29	147.237.0.34	Turkey	tikshuv.idf.il	ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns	7
80.246.130.214	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	6
93.89.19.29	147.237.0.34	Turkey	tikshuv.idf.il	SQL union select - possible sql injection attempt - GET parameter	4
93.89.19.29	147.237.0.34	Turkey	tikshuv.idf.il	SQL declare varchar - possible SQL injection attempt	4
93.89.19.29	147.237.0.34	Turkey	tikshuv.idf.il	INDICATOR-OBFUSCATION large number of calls to char function - possible sql injection obfuscation	4
177.185.194.47	147.237.77.216	Brazil	dover.idf.il	SQL Injection - Select From	4
93.89.19.29	147.237.0.34	Turkey	tikshuv.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UPDATE SET	4
93.89.19.29	147.237.0.34	Turkey	tikshuv.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	4
66.249.93.74	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	4
93.89.19.29	147.237.0.34	Turkey	tikshuv.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	4
66.249.66.131	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
93.89.19.29	147.237.0.34	Turkey	tikshuv.idf.il	SQL url ending in comment characters - possible sql injection attempt	4
93.89.19.29	147.237.0.34	Turkey	tikshuv.idf.il	SQL generic sql update injection attempt - GET parameter	4
209.173.241.141	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	4
93.89.19.29	147.237.0.34	Turkey	tikshuv.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	4
93.89.19.29	147.237.0.34	Turkey	tikshuv.idf.il	ET WEB_SERVER Possible SQL Injection (varchar)	4
209.173.241.141	147.237.77.74	United States	law.idf.il	SQL union select - possible sql injection attempt - GET parameter	3
209.173.241.141	147.237.77.74	United States	law.idf.il	SQL declare varchar - possible SQL injection attempt	3
177.185.194.47	147.237.77.216	Brazil	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	3
209.173.241.141	147.237.77.74	United States	law.idf.il	INDICATOR-OBFUSCATION large number of calls to char function - possible sql injection obfuscation	3
177.185.194.47	147.237.77.216	Brazil	dover.idf.il	SQL generic sql update injection attempt - GET parameter	3
209.173.241.141	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UPDATE SET	3
209.173.241.141	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	3
209.173.241.141	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	3
177.185.194.47	147.237.77.216	Brazil	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	3
177.185.194.47	147.237.77.216	Brazil	dover.idf.il	ET WEB_SERVER Possible SQL Injection (varchar)	3
209.173.241.141	147.237.77.74	United States	law.idf.il	SQL url ending in comment characters - possible sql injection attempt	3
209.173.241.141	147.237.77.74	United States	law.idf.il	SQL generic sql update injection attempt - GET parameter	3
177.185.194.47	147.237.77.216	Brazil	dover.idf.il	SQL union select - possible sql injection attempt - GET parameter	3
177.185.194.47	147.237.77.216	Brazil	dover.idf.il	SQL declare varchar - possible SQL injection attempt	3
209.173.241.141	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	3
177.185.194.47	147.237.77.216	Brazil	dover.idf.il	INDICATOR-OBFUSCATION large number of calls to char function - possible sql injection obfuscation	3
209.173.241.141	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Possible SQL Injection (varchar)	3
177.185.194.47	147.237.77.216	Brazil	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UPDATE SET	3
177.185.194.47	147.237.77.216	Brazil	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	3
177.185.194.47	147.237.77.216	Brazil	dover.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	3
213.8.145.99	147.237.72.166	Israel	aka.idf.il	ET WEB_SPECIFIC_APPS Efkan Forum SQL Injection Attempt -- default.asp id SELECT	2

04-18-2016 to 04-19-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.171.244.115	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	522
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	318
132.66.110.109	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	297
37.26.148.190	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	273
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	243
109.64.127.196	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	222
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	221
50.117.45.133	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	198
176.13.9.164	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	162
212.76.124.149	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	152
104.162.241.87	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	152
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	141
85.130.251.127	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	126
2.53.169.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
198.199.14.52	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	111
46.120.70.96	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	108
198.199.14.54	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
87.71.98.198	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
2.53.170.52	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	94
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
109.65.160.58	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	87
64.216.107.11	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	85
2.53.30.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
176.13.13.50	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
197.231.1.175	Mauritania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
78.65.172.217	Sweden	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	80
176.13.9.164	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	80
66.249.83.242	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
46.120.166.164	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	76
66.249.83.248	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
79.183.168.32	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
87.70.54.152	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
109.67.61.221	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
109.67.194.8	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
198.199.14.53	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
76.180.215.21	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	58
5.22.130.75	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
84.108.238.220	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	56
66.249.83.245	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
193.43.245.250	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
193.43.246.250	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
149.78.54.19	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
5.29.122.211	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
37.124.195.156	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
62.90.184.141	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	43
109.64.146.60	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42

04-18-2016 to 04-19-2016

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
85.64.86.157	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
212.143.99.102	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
24.114.223.254	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
62.219.137.44	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.169.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	314
176.13.9.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	271
46.19.85.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	244
2.55.189.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	239
46.19.85.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	209
46.121.30.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	207
2.53.15.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	182
176.13.8.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	181
46.19.85.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	165
176.13.15.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	149
2.53.58.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	145
46.19.85.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	143
46.19.85.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
2.53.56.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
2.53.40.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
2.53.1.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
176.13.5.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
2.55.12.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
2.53.155.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
176.13.12.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
2.53.190.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
46.19.86.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
185.32.179.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
176.13.0.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
94.159.152.117	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	72
46.19.86.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
109.253.128.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
94.159.152.117	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.159.152.117	Block	68
37.26.146.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
46.19.85.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
80.246.139.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
109.253.224.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
176.13.0.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
2.53.170.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
46.19.85.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
2.53.185.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
2.55.26.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
79.180.116.19	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	54
2.53.37.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
46.19.85.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
217.132.159.36	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 217.132.159.36	Block	50
79.180.116.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
80.246.137.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
37.26.146.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
176.13.14.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
198.199.14.51	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	35
2.55.41.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
80.246.136.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
192.114.5.10	Israel	147.237.76.39	mobile.meitav.idf.il	Distributed Suspicious Response Code	Block	30

04-18-2016 to 04-19-2016