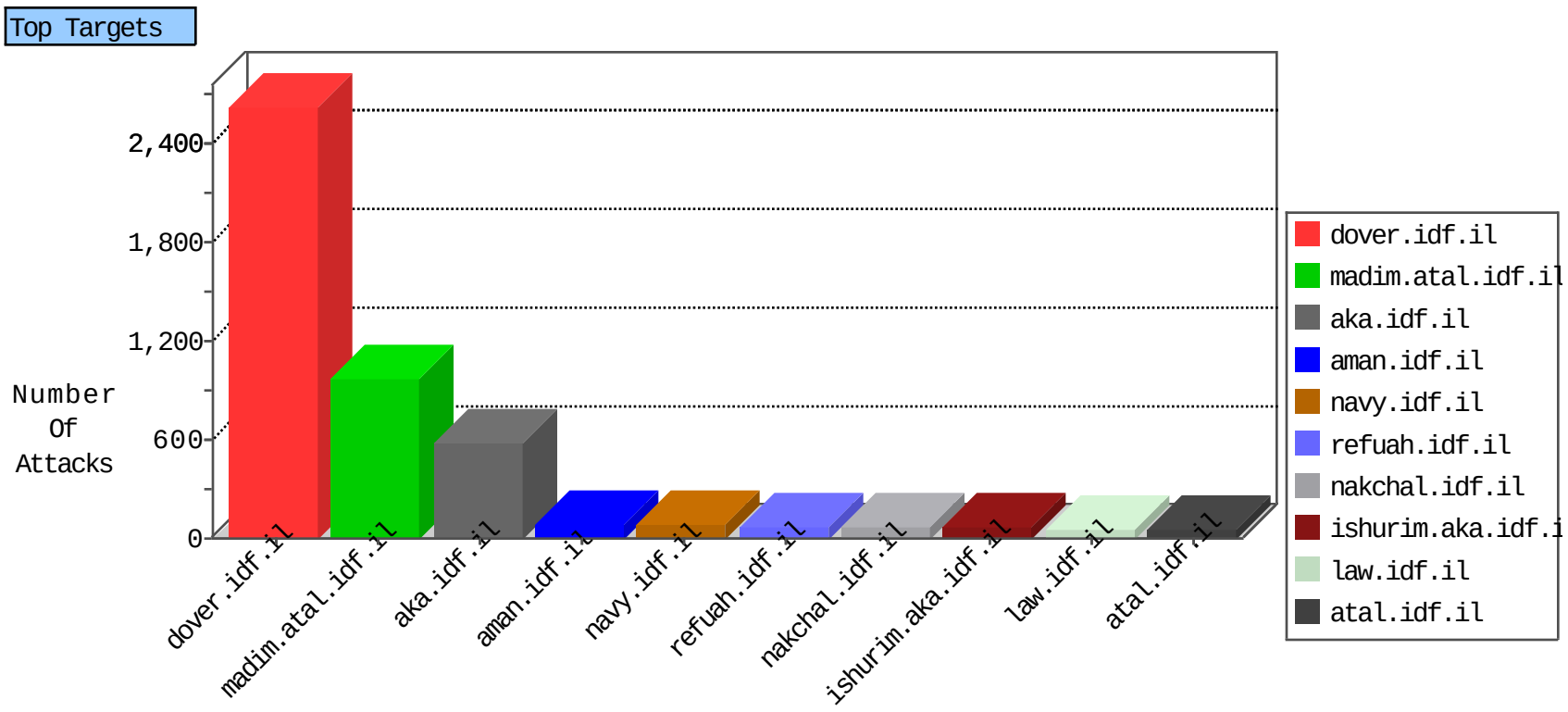
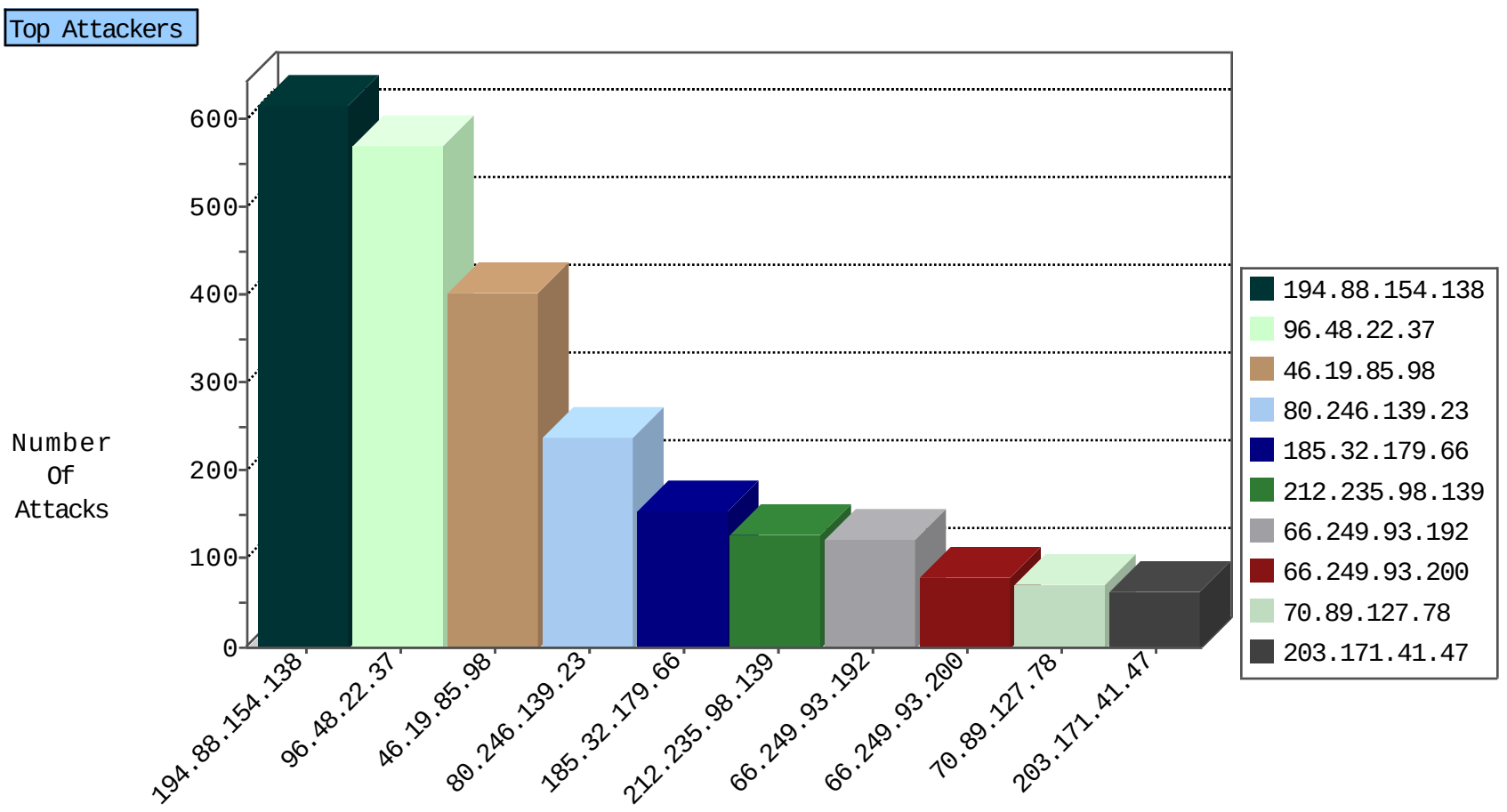
11-23-2015-11:04:09 to 11-23-2015-12:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



11-23-2015-11:04:09 to 11-23-2015-12:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.59.4	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
114.80.122.91	China	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
114.80.122.91	China	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1

11-23-2015-11:04:09 to 11-23-2015-12:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.88.154.138	Poland	147.237.77.216	dover.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	100
194.88.154.138	Poland	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	78
70.89.127.78	United States	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	69
96.48.22.37	Canada	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	63
216.201.148.210	United States	147.237.76.42	refuah.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	19
203.171.41.47	New Zealand	147.237.76.31	nakchal.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	16
178.63.18.196	Germany	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	15
194.88.154.138	Poland	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	10
178.63.18.196	Germany	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
74.63.228.226	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
216.249.104.194	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
216.185.43.135	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
203.171.41.47	New Zealand	147.237.76.31	nakchal.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	7
108.168.219.174	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	7
96.48.22.37	Canada	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
216.201.148.210	United States	147.237.76.42	refuah.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	5
70.89.127.77	United States	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	5
194.88.154.138	Poland	147.237.77.216	dover.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	3
96.48.22.37	Canada	147.237.77.216	dover.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	3
189.38.80.71	Brazil	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
109.186.33.145	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
189.38.80.71	Brazil	147.237.77.233	atal.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1
178.63.18.196	Germany	147.237.76.86	navy.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	1
203.171.41.47	New Zealand	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
66.240.213.93	United States	147.237.0.16	my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
96.48.22.37	Canada	147.237.77.216	dover.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	1
108.168.219.174	United States	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
70.89.127.77	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

11-23-2015-11:04:09 to 11-23-2015-12:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
194.88.154.138	147.237.77.216	Poland	dover.idf.il	SQL Injection - Select From	399
96.48.22.37	147.237.77.216	Canada	dover.idf.il	SQL Injection - Select From	391
178.63.18.196	147.237.76.86	Germany	navy.idf.il	SQL Injection - Select From	39
216.201.148.210	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	32
108.168.219.174	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	20
203.171.41.47	147.237.76.31	New Zealand	nakchal.idf.il	SQL Injection - Select From	15
74.63.228.226	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
189.38.80.71	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	7
216.249.104.194	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	5
46.228.207.18	147.237.8.14	Germany	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.13.192	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.84.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
108.168.219.174	147.237.77.74	United States	law.idf.il	ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns	1
23.95.248.139	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
213.41.72.13	147.237.77.216	France	dover.idf.il	GPL SCAN nmap TCP	1
96.48.22.37	147.237.77.216	Canada	dover.idf.il	ET WEB_SERVER SQLi - SELECT and sysobject	1
2.52.130.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
206.169.53.122	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
81.137.211.61	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
80.178.169.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
74.117.209.136	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.253	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.19.86.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.151.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
108.168.219.174	147.237.77.74	United States	law.idf.il	ET WEB_SERVER SQLi - SELECT and sysobject	1
23.95.248.139	147.237.77.233	United States	atal.idf.il	ET SCAN Potential SSH Scan	1
216.201.148.210	147.237.76.42	United States	refuah.idf.il	ET WEB_SERVER SQLi - SELECT and sysobject	1
23.95.248.139	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
212.143.3.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
96.48.22.37	147.237.77.216	Canada	dover.idf.il	ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns	1
206.169.53.122	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.101.186.178	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
79.180.143.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
182.105.104.14	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1

11-23-2015-11:04:09 to 11-23-2015-12:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	128
96.48.22.37	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	105
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
92.90.20.27	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
123.103.8.180	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	37
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
194.88.154.138	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
2.52.131.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
203.171.41.47	New Zealand	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	24
66.249.82.91	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
194.206.156.229	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
138.134.192.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	22
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
217.6.221.183	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
52.34.138.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
123.103.8.180	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.85.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
82.113.106.151	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
80.215.192.91	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
37.26.146.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
213.6.150.158	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
100.100.14.151		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
100.100.82.169		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	13
66.249.93.200	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
152.62.109.209	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
104.131.200.249	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
77.125.163.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
107.170.62.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.255.206.193	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.238	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
66.249.93.200	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
100.100.85.199		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
212.117.151.42	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.184	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
66.249.82.94	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.238	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.200	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
85.214.11.209	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9

11-23-2015-11:04:09 to 11-23-2015-12:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	196
80.246.139.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	127
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	100
80.246.139.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
185.32.179.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	82
185.32.179.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
2.54.31.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
176.13.11.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
80.246.139.23	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 80.246.139.23	Block	22
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
80.246.139.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
80.246.136.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.143.3.44	Block	7
84.110.53.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.16.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
185.32.179.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
37.26.146.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.26.146.219	Block	5
212.143.3.44	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	4
46.19.85.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.41.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.190.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.162.91	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
185.32.179.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.143.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.14.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.136.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
5.175.192.24	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.175.192.24	Block	2
46.19.86.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
132.70.66.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
2.54.63.70	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.15.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.186.33.145	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
5.102.224.147	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/ufi/reaction/	Block	1
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
141.212.122.96	United States	147.237.77.226	www.chamatz.aka.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
37.26.148.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
176.12.139.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.13.113.83	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.199.169.20	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.85.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.186.33.145	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/4/	Block	1
2.54.190.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

11-23-2015-11:04:09 to 11-23-2015-12:04:09