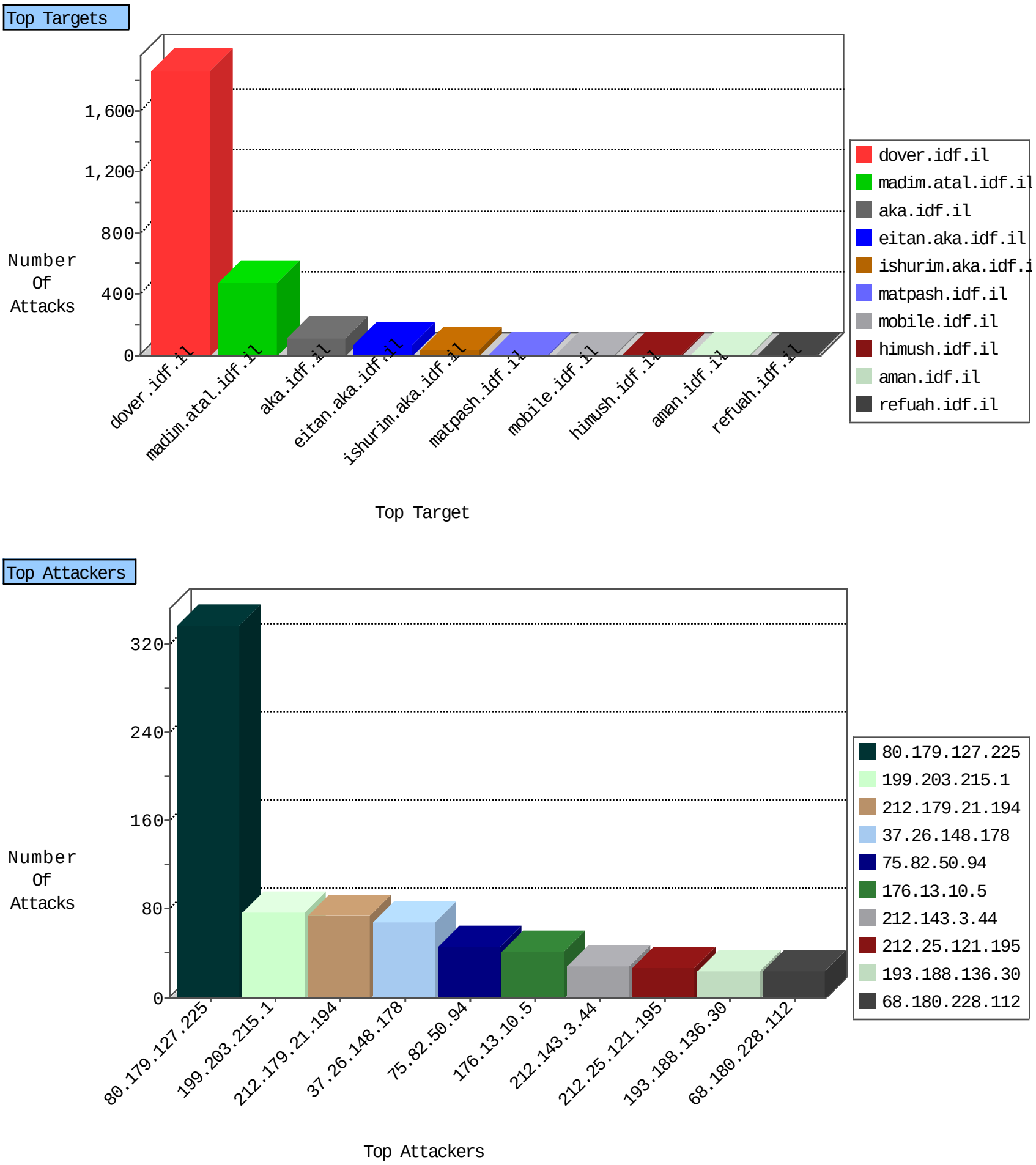
11-09-2015-08:04:08 to 11-09-2015-09:04:08

IDF Under Attack Daily Report



11-09-2015-08:04:08 to 11-09-2015-09:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	27
150.140.136.68	Greece	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
218.38.14.4	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
95.228.150.73	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
204.38.57.82	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
140.113.35.93	Taiwan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
129.15.224.10	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
69.43.37.83	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
193.34.68.7	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
158.75.3.16	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
200.201.25.11	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
188.39.66.125	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
212.43.65.85	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
131.111.81.54	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
165.246.154.3	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
66.124.250.124	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
92.103.236.51	France	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
201.22.148.42	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
76.246.114.73	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
188.211.235.101	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
121.154.105.108	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
168.122.40.11	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
82.198.171.100	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
165.246.154.10	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
66.198.224.2	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
157.193.111.97	Belgium	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
168.122.46.11	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
210.112.120.3	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
142.25.92.3	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
158.108.249.29	Thailand	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
64.57.180.16	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
157.158.16.120	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
61.100.11.2	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
121.66.75.123	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
190.64.49.52	Uruguay	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
136.199.217.122	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
12.147.136.38	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
209.98.225.211	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	3
83.166.223.6	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
142.151.128.7	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
193.34.70.1	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
91.236.164.21	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
128.197.238.98	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
142.58.248.33	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
66.220.2.2	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
158.108.102.3	Thailand	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
211.25.188.66	Malaysia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
131.188.14.7	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
140.117.72.3	Taiwan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
121.124.127.6	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2

11-09-2015-08:04:08 to 11-09-2015-09:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.160.240.11	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.20.69.74	United States	147.237.77.179	e.mazi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

11-09-2015-08:04:08 to 11-09-2015-09:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.98.225.211	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sA (2)	1
198.20.69.74	147.237.77.179	United States	e.mazi.idf.il	ET DROP Dshield Block Listed Source	1
176.13.5.208	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.226.133	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.189.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.67.240	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
64.39.102.107	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.98.225.211	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sA (2)	1
5.189.171.83	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
205.237.196.2	147.237.77.216	United States	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
94.230.86.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.138.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.88.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.67.232	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
46.172.71.250	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.64.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

11-09-2015-08:04:08 to 11-09-2015-09:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
199.203.215.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
75.82.50.94	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
212.143.3.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
193.188.136.30	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
5.29.51.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
120.20.150.194	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
149.78.111.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
50.179.141.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
77.126.88.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
80.179.90.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
207.244.89.75	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
31.154.94.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
147.236.38.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
40.77.167.9	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.122.187		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
212.117.136.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.80.51.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
185.3.144.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
79.181.196.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.116.210.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.2.62.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
81.218.251.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
213.8.99.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.148.210	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
95.86.106.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.120.126.59		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
73.223.21.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
164.2.255.244	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
134.191.232.72	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.12.147.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
31.168.99.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.122.154.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.148.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
195.189.210.188	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
81.218.101.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

11-09-2015-08:04:08 to 11-09-2015-09:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.179.127.225	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.179.127.225	Block	170
80.179.127.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	168
37.26.148.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	44
176.13.10.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
2.52.22.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
213.8.81.18	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 213.8.81.18	Block	18
77.126.37.66	Israel	147.237.72.166	aka.idf.il	Multiple Double URL Encoding from 77.126.37.66	Block	4
46.19.85.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.144.49.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.254	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	3
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.4.41	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.142.68.27	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
195.182.75.7	Lithuania	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/en	Block	2
84.228.156.61	Israel	147.237.0.16	my-kosher-kravi.idf.il	Parameter Type Violation Master$ContentPlaceHolder1$password in my-kosher-kravi.idf.il/templates/login/login.aspx	Block	2
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
195.189.210.188	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 195.189.210.188	Block	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
2.54.27.66	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
222.240.124.199	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.67.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
193.188.136.30	Lebanon	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.157	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8944-he/refuah.aspx	Block	1
85.65.83.96	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
77.126.37.66	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
66.249.67.138	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
198.20.69.74	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
184.105.247.195	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
46.19.85.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/valtam	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
194.90.219.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pniasubmittedsuccessfully.aspx	None	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
37.26.149.216	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.88.102.43	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.67.147	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/	Block	1
212.76.99.212	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.32.179.233	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.136.172	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71559-he/maarachot.aspx	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
194.90.219.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
176.12.146.207	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
66.249.67.232	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
188.165.15.234	France	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
46.19.86.201	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.81.17.28	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/1/size338x0/1531.jpg	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1

11-09-2015-08:04:08 to 11-09-2015-09:04:08