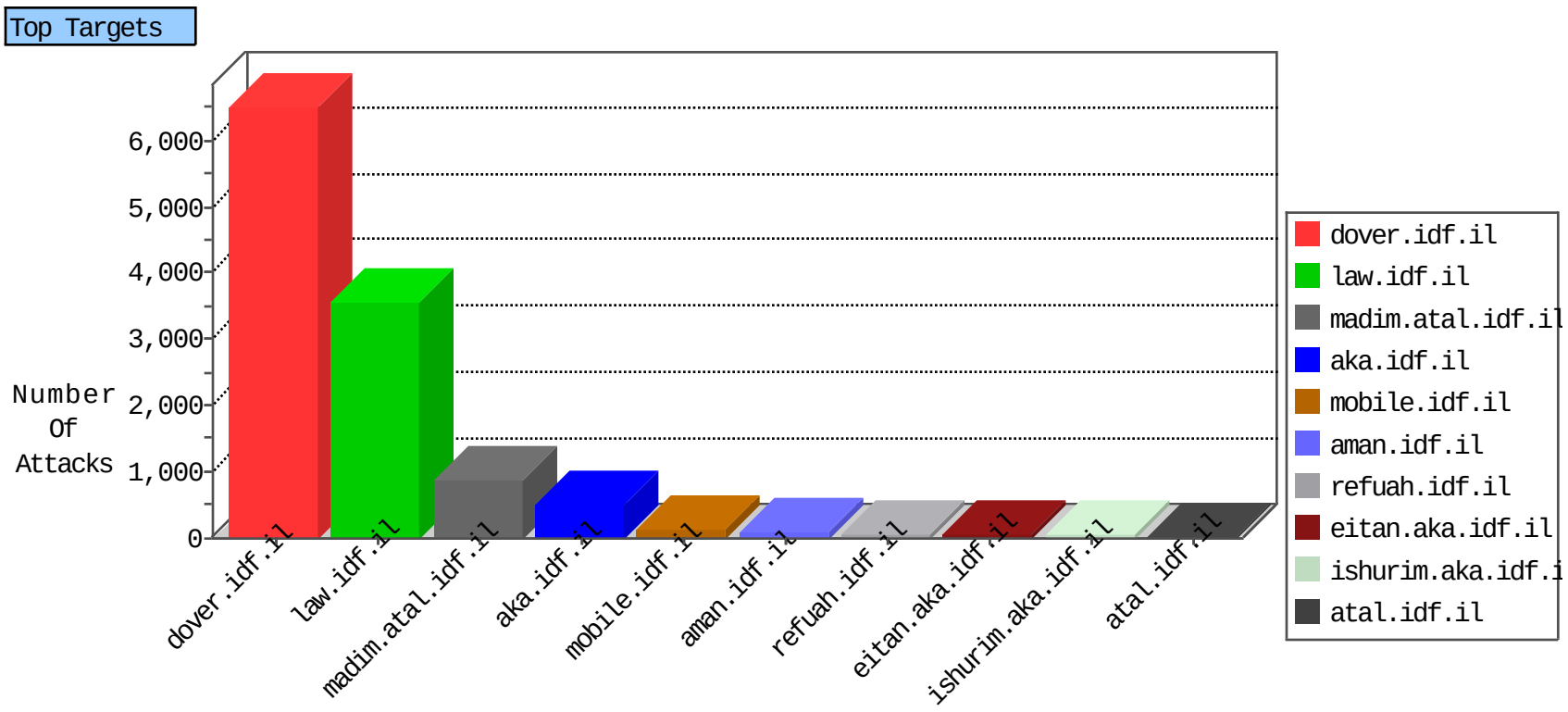
12-28-2015-12:04:03 to 12-28-2015-13:04:03

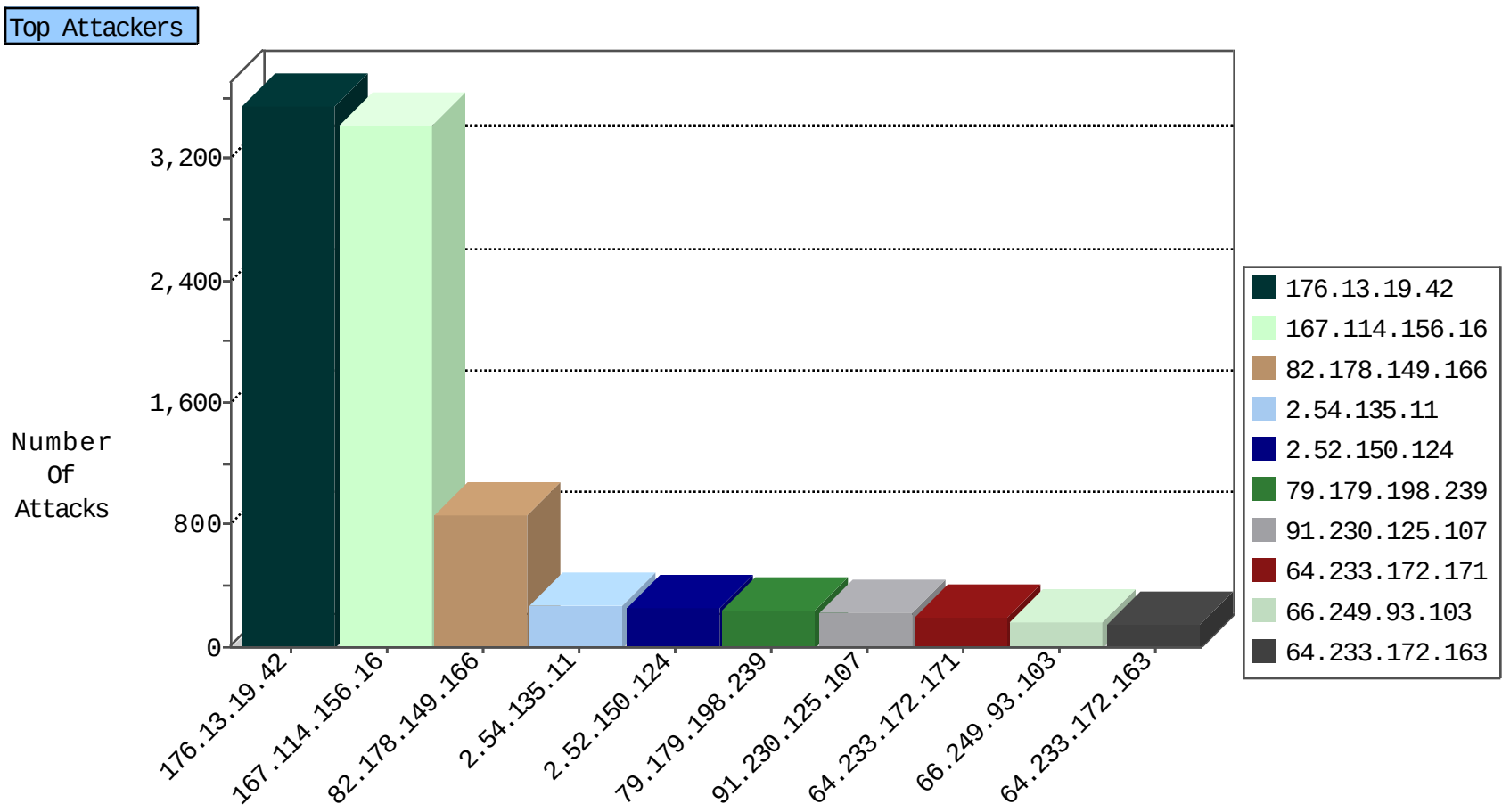
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-28-2015-12:04:03 to 12-28-2015-13:04:03

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	DOS-Tool-SwitchbladG	dest-reset	3124
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1116
82.178.149.166	Oman	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	838
91.230.125.107	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	483
66.249.93.103	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	134
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
66.249.93.107	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	103
66.249.93.99	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	96
66.249.78.159	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	76
66.249.78.166	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	45
91.230.125.107	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	43
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	36
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	21
188.247.74.5	Jordan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
204.13.200.200	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
115.78.114.229	Vietnam	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
107.178.194.79	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
66.249.66.28	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
213.55.114.234	Ethiopia	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
176.13.19.42	Israel	147.237.77.74	law.idf.il	network flood IPv4 TCP-RST	drop	12
50.153.163.46	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
66.249.66.31	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
37.26.146.248	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
193.200.241.195	Germany	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
85.10.210.199	Germany	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
148.177.129.212	Europe	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
82.114.168.158	Yemen	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
85.10.210.199	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
107.178.194.87	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
65.19.138.34	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
84.14.218.114	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
213.55.114.234	Ethiopia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
64.233.172.163	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
182.73.13.118	India	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
82.178.149.166	Oman	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	6
104.131.240.186	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
66.249.78.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
107.170.91.224	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
89.169.98.152	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
162.243.57.54	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
115.78.114.229	Vietnam	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
198.58.103.102	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
66.102.9.91	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
37.26.146.248	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4

12-28-2015-12:04:03 to 12-28-2015-13:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.163.222.10	Germany	147.237.77.216	dover.idf.il	19863: HTTP: WordPress Revslider/Showbiz PHP File Upload	Block	3

12-28-2015-12:04:03 to 12-28-2015-13:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.178.149.166	147.237.77.216	Oman	dover.idf.il	SERVER-APACHE Apache SSI error page cross-site scripting	447
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
109.253.156.95	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
109.253.156.95	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
94.102.48.195	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.189.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.47.229.34	147.237.77.234	France	halag.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.160.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.2.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.103	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.63	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.85.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.55	147.237.8.28		e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.253.212.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.198.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
223.194.199.9	147.237.72.156	Korea, Republic of	aman.idf.il	ET SCAN Potential SSH Scan	1
79.182.138.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.17.168	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.63	147.237.76.176		test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.78.158	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
151.217.178.63	147.237.0.19		madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.85.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.70.66.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

12-28-2015-12:04:03 to 12-28-2015-13:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.19.42	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1865
176.13.19.42	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1658
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1249
82.178.149.166	Oman	147.237.77.216	dover.idf.il	drop	SAM rule	drop	238
82.178.149.166	Oman	147.237.77.216	dover.idf.il	drop		drop	74
64.233.172.171	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	37
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
64.233.172.171	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	37
64.233.172.171	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
64.233.172.171	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	37
64.233.172.163	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
64.233.172.163	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	32
64.233.172.163	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	32
79.178.171.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
85.250.119.203	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.0.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	29
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
147.236.232.254	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
64.233.172.155	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
64.233.172.155	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	23
64.233.172.155	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
64.233.172.155	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
82.145.211.18	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
64.233.172.163	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
46.19.85.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
79.182.197.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
82.81.9.134	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.85.46	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
2.52.150.124	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.52.150.124	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
212.143.40.198	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
66.249.93.103	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
66.249.93.99	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
149.88.251.52	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.54.243	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
118.71.105.107	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.150.124	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.19.86.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.16.5.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.52.150.124	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
66.249.93.99	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
66.249.93.107	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10

12-28-2015-12:04:03 to 12-28-2015-13:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.135.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	130
79.179.198.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	128
2.52.150.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	125
2.54.135.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	111
79.179.198.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	107
2.52.150.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	59
46.19.85.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
37.26.147.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
2.54.135.11	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.135.11	Block	24
46.19.85.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
176.13.0.248	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
37.26.147.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
46.19.85.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
82.166.61.61	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
46.19.86.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.4.136	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
185.32.179.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.142	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.133.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	3
2.54.168.166	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.13.19.9	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	2
176.13.4.151	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.108.103.220	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
212.179.146.134	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
94.230.93.162	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	2
37.142.64.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.105	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
31.168.23.60	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.60	Block	2
2.52.150.124	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.133.159	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1390	Block	2
176.13.18.194	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	2
2.54.59.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.179.15.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
31.168.118.146	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.116.208.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
2.54.61.124	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
79.177.182.79	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.133.169	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/69039.pdf	Block	1
149.78.214.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.149.195	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.139.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	1
37.26.146.172	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method uÂ¯Â¸ ^ÃˆÃ£'Â?Â..Ã»FÂ'Ã¿Ã¡[[#20]]Â¯[[#5]]Â-[[#23]]_[[#14]]Ã¯Ã²Â, Ã¹ÂµÂ Ã©Jl in URL	Block	1

12-28-2015-12:04:03 to 12-28-2015-13:04:03