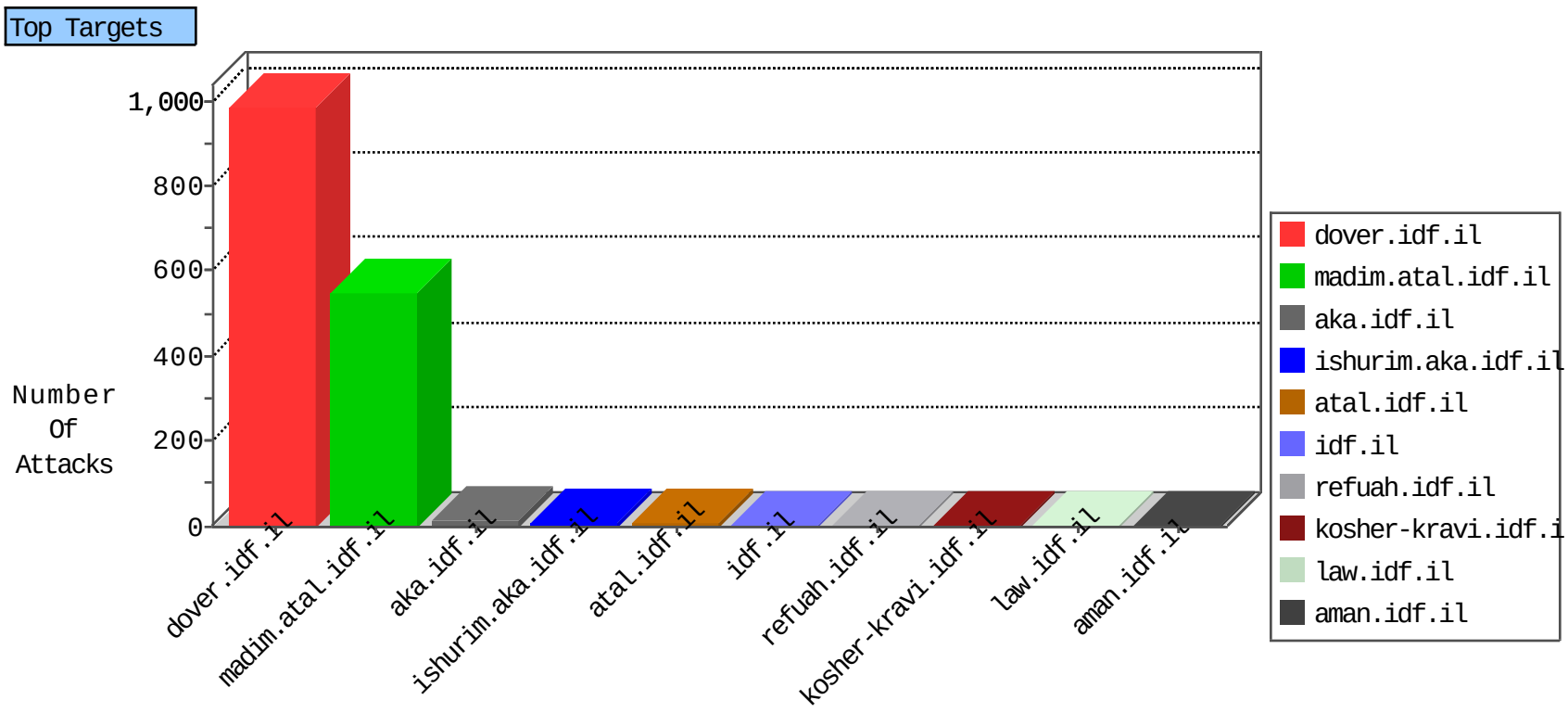
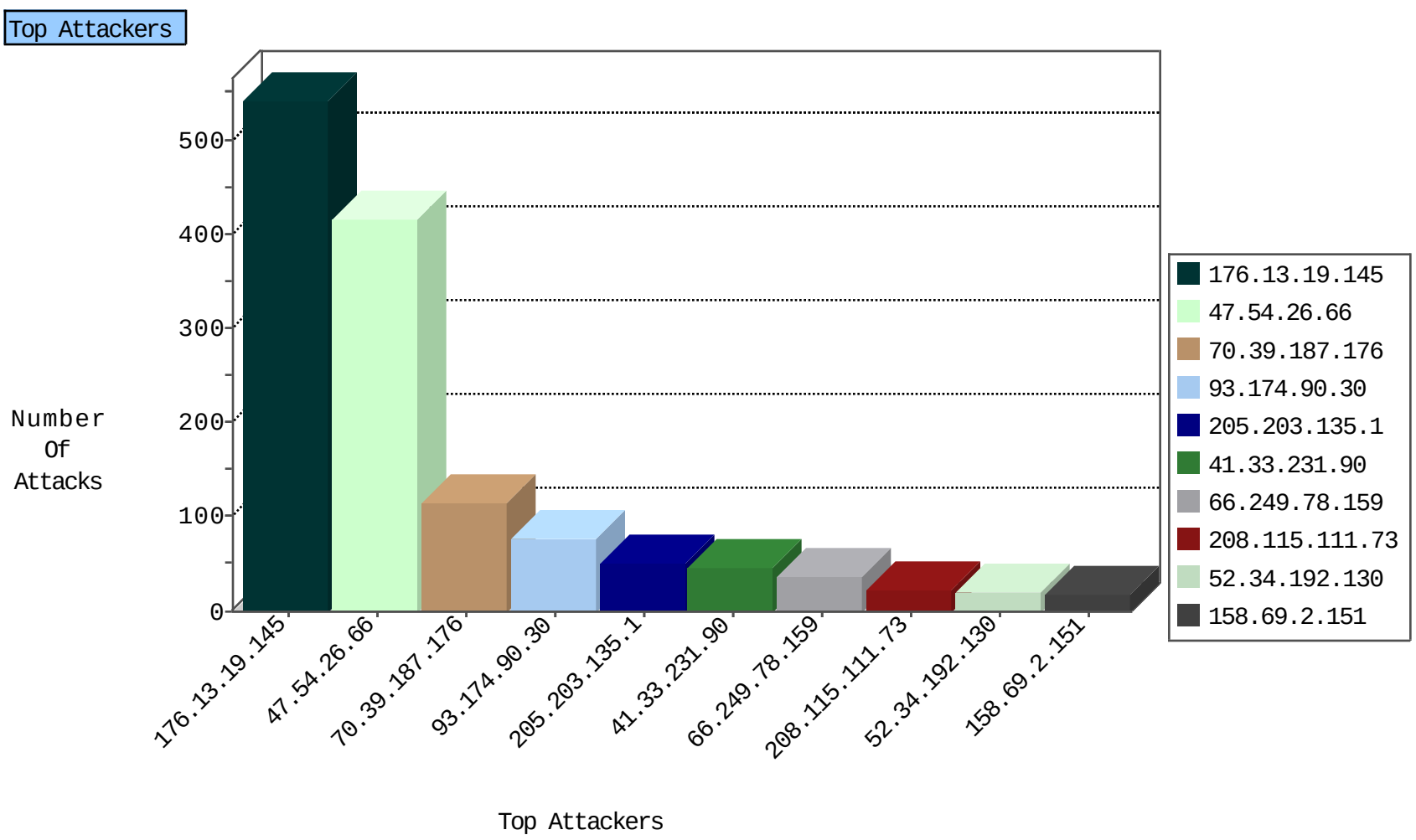
11-22-2015-04:04:03 to 11-22-2015-05:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-22-2015-04:04:03 to 11-22-2015-05:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.190	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	410
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	7
115.231.222.40	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Http	drop	2
61.147.103.92	China	147.237.0.33	idf.il	Frk_Under_Attack_Con_Tcp	drop	2

11-22-2015-04:04:03 to 11-22-2015-05:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.242.198	Canada	147.237.76.38	e.e.meitav.idf.i	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1

11-22-2015-04:04:03 to 11-22-2015-05:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
94.102.48.195	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
31.6.71.154	147.237.77.216	Poland	dover.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.77.74	Sweden	law.idf.il	ET SCAN NMAP -sS window 1024	1
159.122.238.133	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 2048	1
141.105.71.68	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
101.22.189.167	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
74.117.209.136	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
31.6.71.154	147.237.76.200	Poland	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.77.243	Sweden	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
188.214.128.12	147.237.0.33	Romania	idf.il	ET SCAN NMAP -sS window 1024	1
159.122.238.133	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -f -sS	1
141.105.71.68	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

11-22-2015-04:04:03 to 11-22-2015-05:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
47.54.26.66	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	415
70.39.187.176	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
93.174.90.30	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
52.34.192.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
158.69.2.151	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.196	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	10
87.203.103.152	Greece	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	9
157.55.39.75	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.145	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
157.55.39.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
70.198.209.105	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
173.68.68.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
99.249.124.181	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
162.209.84.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.19.145	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
76.26.11.68	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
40.77.167.63	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
61.135.190.71	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
162.209.102.100	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.167.63	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
64.236.82.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
208.115.111.73	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
166.78.9.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.132	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
166.78.134.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
94.200.52.18	United Arab Emirates	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
76.26.11.68	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.159	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
150.108.240.30	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.19.145	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid sequence number	alert	2
5.22.129.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.159	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
52.28.32.164	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
122.224.8.111	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

11-22-2015-04:04:03 to 11-22-2015-05:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.19.145	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.19.145	Block	364
176.13.19.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	169
129.184.84.40	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	6
176.13.19.145	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.19.145	Block	3
176.12.142.230	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
176.12.148.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
46.19.85.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
184.172.57.52	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-admin/	Block	1
157.55.39.142	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
74.6.53.183	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/test/wp-admin/	Block	1
176.13.19.145	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19795-he/idfgdover.aspx	Block	1
157.55.39.229	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/drushim/faq.aspx	None	1
79.182.125.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
61.135.190.69	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20493-he/dover.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
93.174.90.30	Netherlands	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
61.135.190.71	China	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
129.184.84.40	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
61.135.190.198	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1559-en/kkkkkkk=2e18845bkkkkkkk_2e18845b	Block	1
157.55.39.142	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/results.asp	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
46.19.86.208	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie _pk_ref.322.9cd2: Expected ["","",1446980080,"https://www.google.co.il/"], Observed ["","",1448158973,"https://www.google.co.il/"]	None	1
212.199.57.207	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.x in www.idf.il/1842-he/dover.aspx	Block	1

11-22-2015-04:04:03 to 11-22-2015-05:04:03