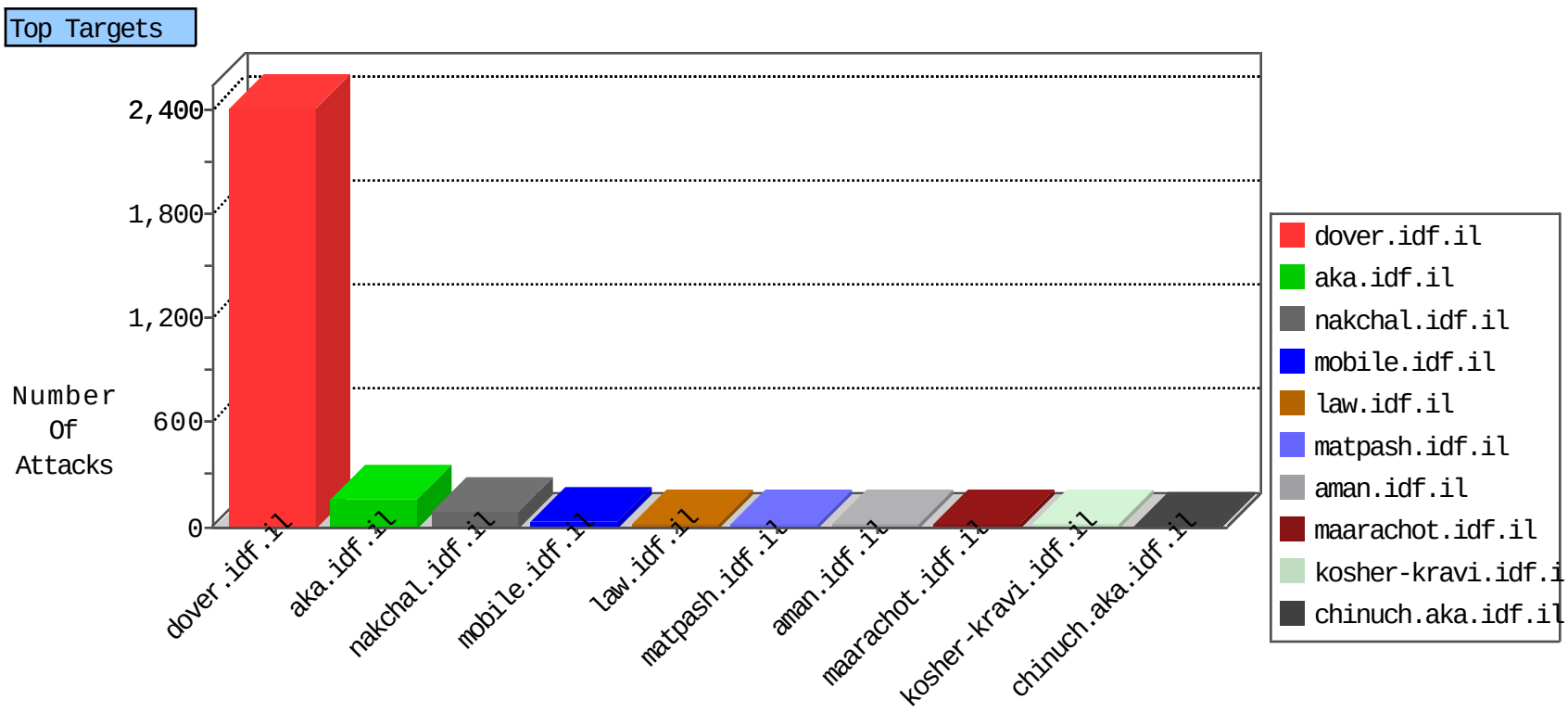
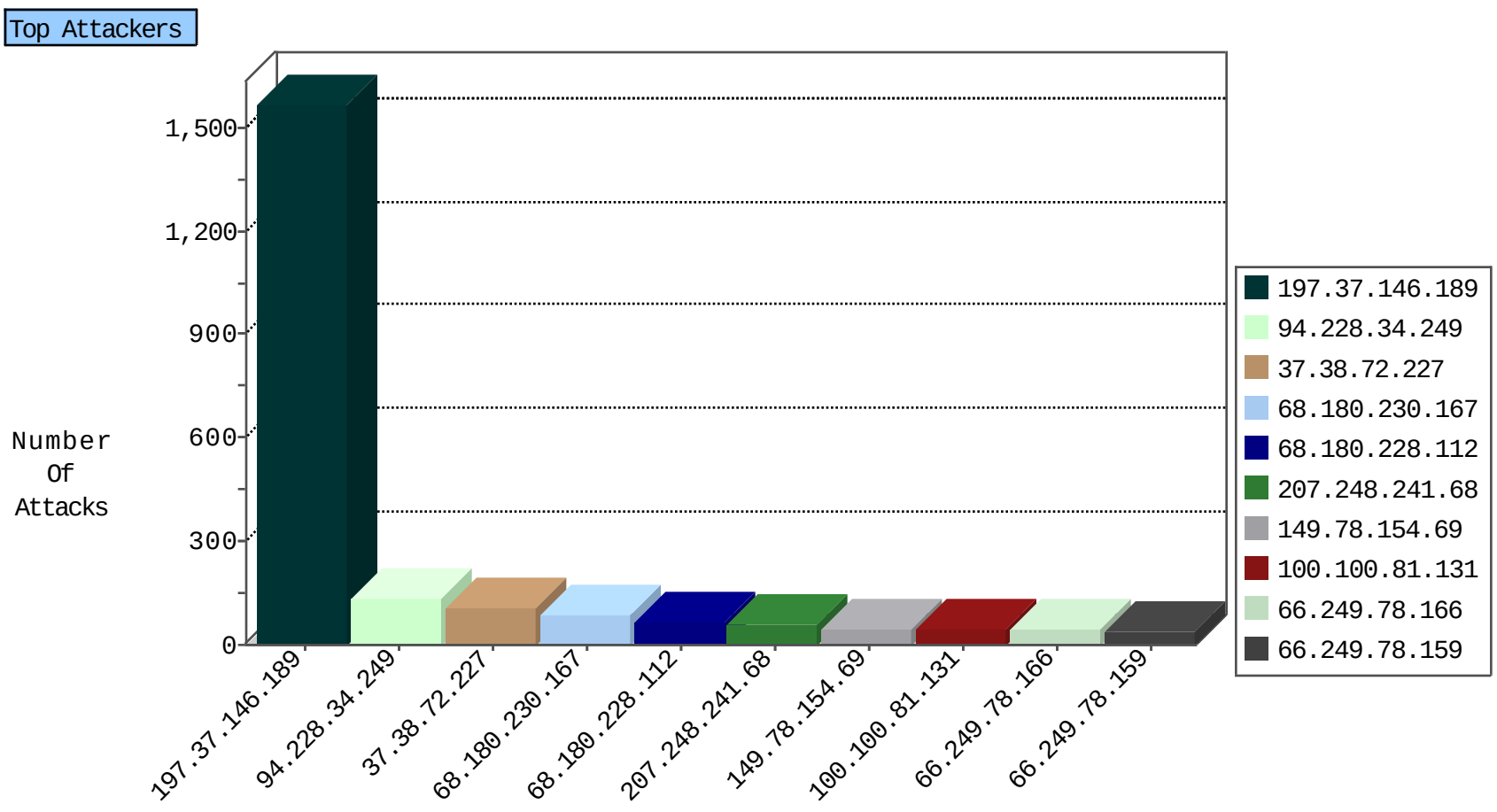
10-28-2015-02:04:07 to 10-28-2015-03:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-28-2015-02:04:07 to 10-28-2015-03:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
222.186.21.180	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
220.255.146.30	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-28-2015-02:04:07 to 10-28-2015-03:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-28-2015-02:04:07 to 10-28-2015-03:04:07

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
59.45.79.117	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
94.102.63.7	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.63.7	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
94.102.49.102	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.49.102	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
89.248.171.19	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
62.210.25.83	147.237.76.200	France	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
5.238.223.147	147.237.76.31	Iran, Islamic Republic of	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.143.123.180	147.237.0.19	Brazil	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
121.12.127.94	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
94.102.63.7	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
94.102.63.7	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
94.102.49.102	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
89.248.171.19	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
87.4.67.173	147.237.76.31	Italy	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
62.210.25.83	147.237.76.200	France	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
121.12.127.94	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

10-28-2015-02:04:07 to 10-28-2015-03:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1387
94.228.34.249	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	drop		drop	122
37.38.72.227	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
207.248.241.68	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
100.100.81.131		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	47
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
66.249.78.159	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	SAM rule	drop	24
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
98.206.24.169	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.64.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
121.7.37.167	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	7
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
119.73.253.5	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
166.78.134.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.44.224.86	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
203.127.96.200	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
119.73.253.5	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
157.55.39.55	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
50.203.151.94	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	4
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.97.52.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
203.127.96.200	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
184.173.183.174	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.167.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.177.162.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.186.28.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.168.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
162.209.84.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
105.196.16.64	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.12.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

10-28-2015-02:04:07 to 10-28-2015-03:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1111-he/nakhal.aspx	Block	84
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	56
85.64.205.157	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 85.64.205.157	Block	28
2.52.19.197	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	28
61.135.190.71	China	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	14
189.175.137.65	Mexico	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list.htm	Block	14
93.155.253.164	Bulgaria	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	14
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on 147.237.77.170/robots.txt	Block	14
77.126.22.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
141.212.122.160	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	14
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18189-he/dover.aspx	Block	14
157.55.39.140	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar/	Block	14
85.65.98.228	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
31.193.51.78	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
188.165.15.205	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-5834-he/patzar.aspx	Block	14
93.155.253.164	Bulgaria	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 93.155.253.164 (Open Mode)	None	14

10-28-2015-02:04:07 to 10-28-2015-03:04:07