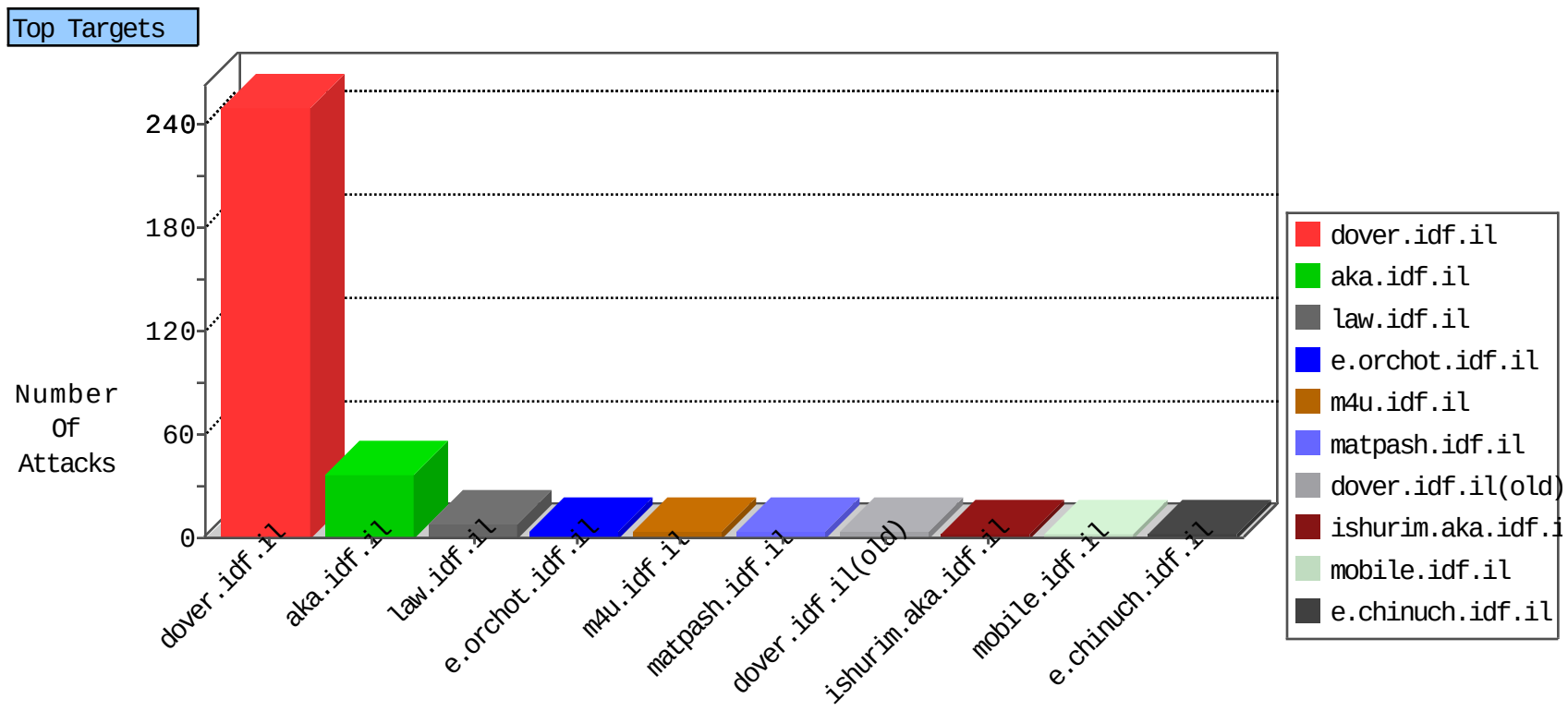
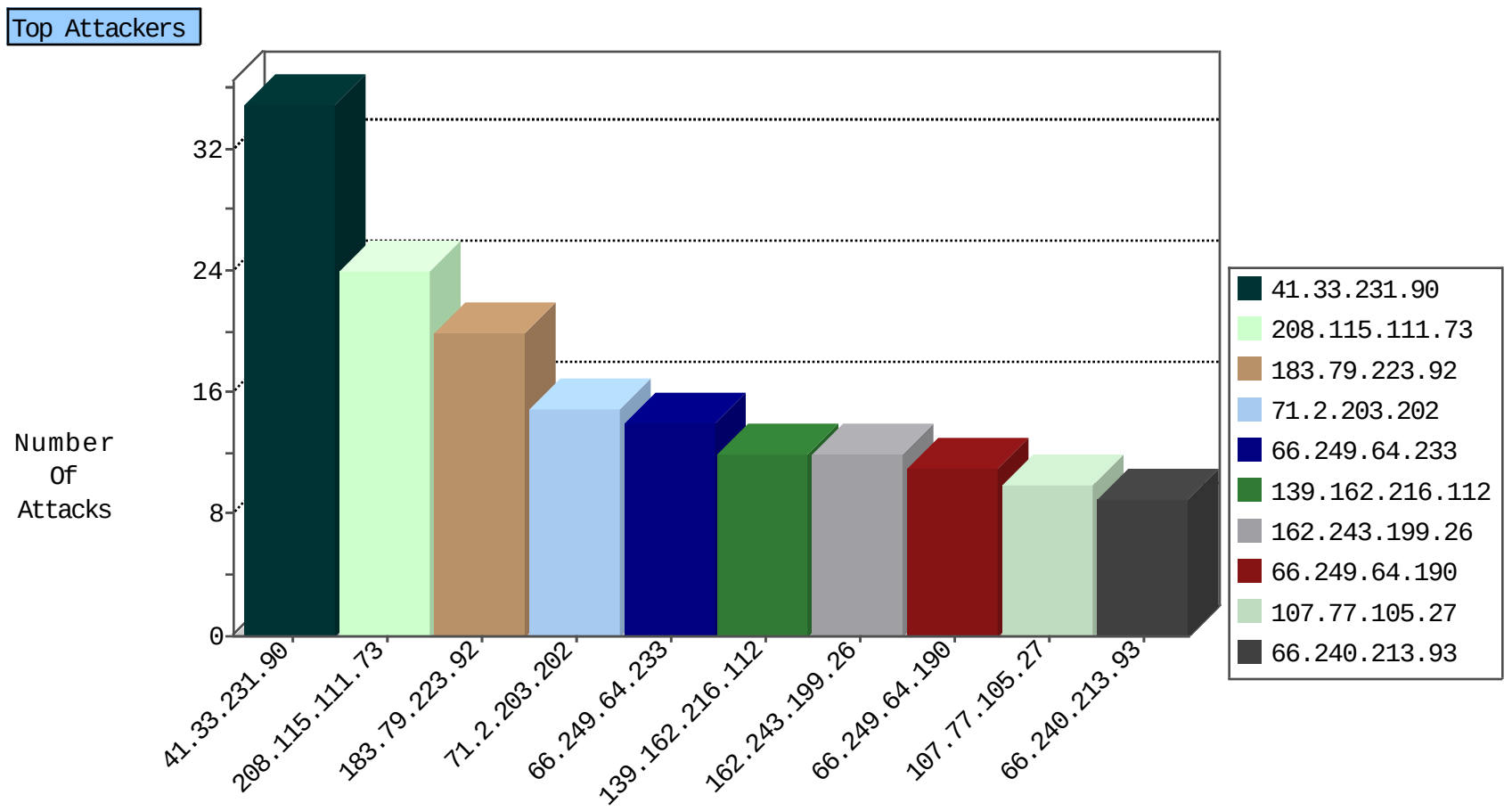
11-23-2015-02:04:10 to 11-23-2015-03:04:10

IDF Under Attack
Daily Report

Top Targets



Top Attackers



11-23-2015-02:04:10 to 11-23-2015-03:04:10

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.200	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	404
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
185.106.94.57		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
142.4.193.203	United States	147.237.76.38	e.e.meitav.idf.i	Block_Ntp_All_Net	drop	1
185.106.94.57		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.146	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
176.123.29.13	Moldova, Republic of	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
141.212.122.159	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

11-23-2015-02:04:10 to 11-23-2015-03:04:10

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.240.213.93	United States	147.237.77.179	e.mazi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
66.240.213.93	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
195.154.162.140	France	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

11-23-2015-02:04:10 to 11-23-2015-03:04:10

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
90.44.93.107	147.237.8.14	France	e.orchot.idf.il	ET SCAN Potential SSH Scan	4
90.44.93.107	147.237.8.46	France	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
46.19.85.158	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	2
89.219.56.200	147.237.8.50	Estonia	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
66.240.213.93	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
62.38.250.31	147.237.72.14	Greece	dover.idf.il(old	ET SCAN NMAP -sS window 2048	1
62.38.250.31	147.237.72.14	Greece	dover.idf.il(old	ET SCAN NMAP -f -sS	1
189.254.90.133	147.237.72.166	Mexico	aka.idf.il	ET SCAN NMAP -sS window 4096	1
189.254.90.133	147.237.72.166	Mexico	aka.idf.il	ET SCAN NMAP -f -sS	1
74.117.209.136	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
62.38.250.31	147.237.72.14	Greece	dover.idf.il(old	ET SCAN NMAP -sS window 1024	1
190.3.5.47	147.237.0.34	Argentina	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
189.254.90.133	147.237.72.166	Mexico	aka.idf.il	ET SCAN NMAP -sS window 2048	1

11-23-2015-02:04:10 to 11-23-2015-03:04:10

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
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	23
71.2.203.202	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
183.79.223.92	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.199.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
107.77.105.27	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
130.203.136.75	United States	147.237.77.74	law.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
198.58.99.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
187.243.220.51	Mexico	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
131.253.25.143	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
183.79.223.92	Japan	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.159.104	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
178.255.215.87	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
193.124.251.169	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.253	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.23.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.102.254.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	3
79.178.101.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.87	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.147.205	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
195.154.200.115	France	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
157.55.39.253	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
90.174.2.183	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
65.19.138.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.196.93.147	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.12.144.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.147.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
188.120.148.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.78.10.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
66.240.213.93	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.94.18.203	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
112.74.67.109	China	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.240.213.93	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.94.18.203	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
112.74.67.109	China	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.177.118.201	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.240.213.93	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.121.206	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

11-23-2015-02:04:10 to 11-23-2015-03:04:10

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	3
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
195.154.162.140	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
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	2
66.249.67.31	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
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	2
95.86.64.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.45.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
150.70.173.50	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
213.57.207.59	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
183.79.223.92	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jenin.stm" target="_blank	Block	1
95.108.158.144	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.3	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/maavarrachel.aspx	Block	1
207.46.13.17	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
150.70.173.50	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
213.57.225.109	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 213.57.225.109 (Unknown SSL Session)	None	1
195.154.162.140	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 195.154.162.140	Block	1
66.249.64.17	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/coordinationgaza/governmentrrepresentative/pages/madorarbel.aspx	Block	1
207.46.13.17	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14816-he/dov	Block	1
164.138.126.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
213.57.225.109	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
183.79.223.92	Japan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
80.178.24.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.225.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.154.162.140	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
124.73.1.18	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 124.73.1.18	Block	1
183.79.223.92	Japan	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 183.79.223.92	Block	1

11-23-2015-02:04:10 to 11-23-2015-03:04:10