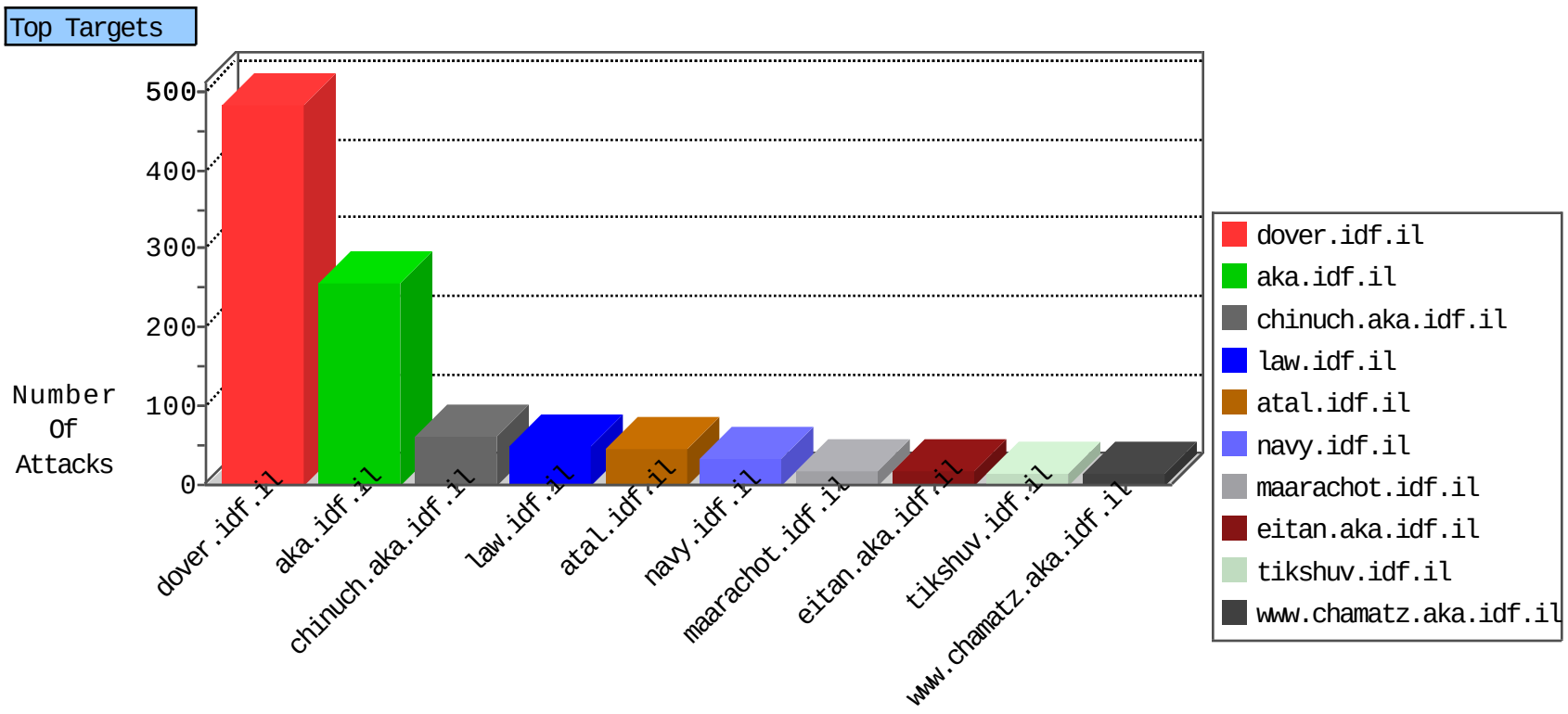
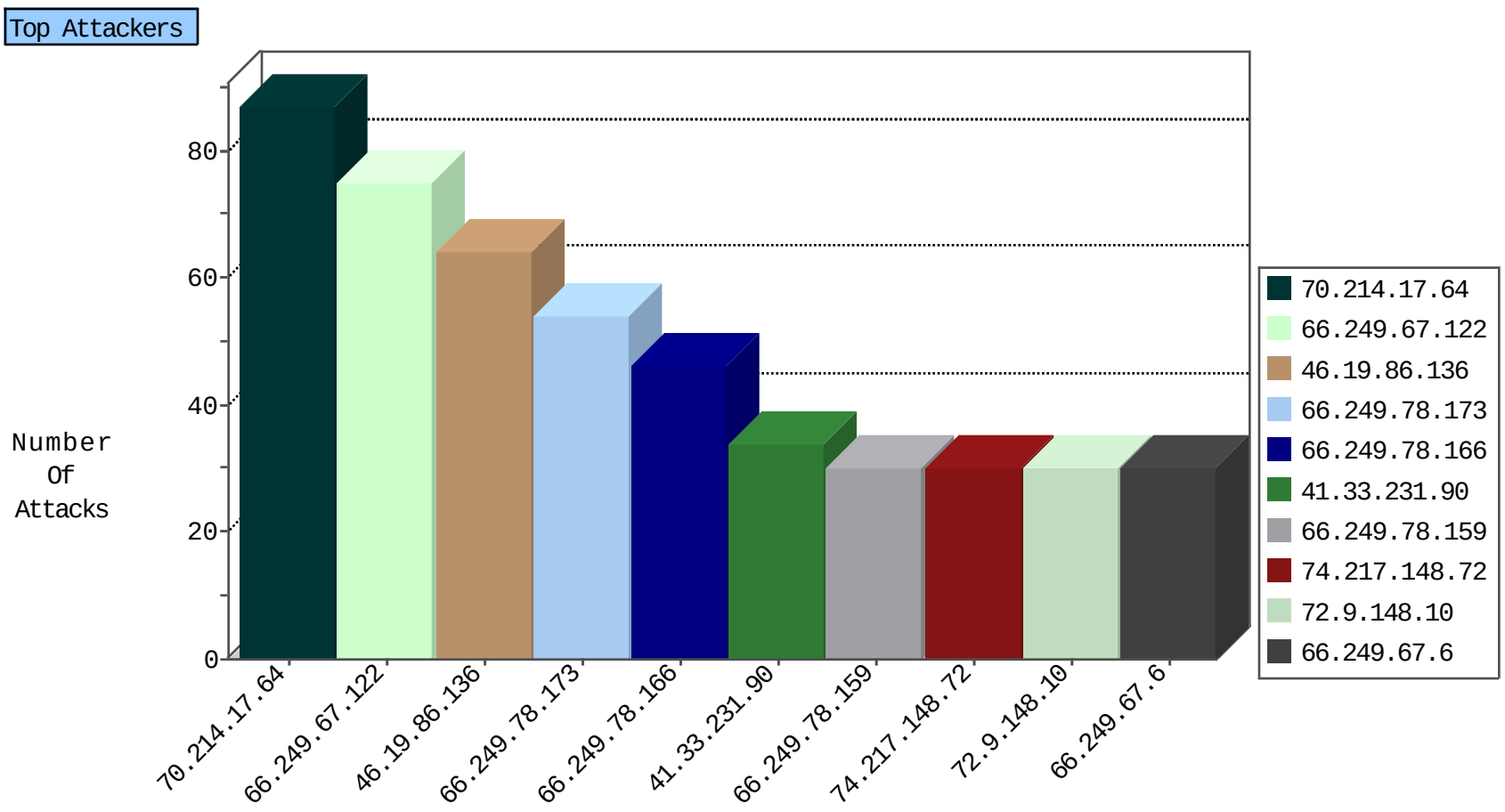
10-31-2015-05:04:00 to 10-31-2015-06:04:00

IDF Under Attack
Daily Report



Top Target



Top Attackers

10-31-2015-05:04:00 to 10-31-2015-06:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6042
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3134
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	466
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	340
151.80.31.112	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	90
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	4
81.218.235.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.161.98.23	Russian Federation	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
121.40.213.227	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
222.186.21.180	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
62.210.148.246	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
91.228.127.198	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
85.25.43.94	Germany	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
46.116.206.159	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
91.228.127.198	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-31-2015-05:04:00 to 10-31-2015-06:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-31-2015-05:04:00 to 10-31-2015-06:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

10-31-2015-05:04:00 to 10-31-2015-06:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
70.214.17.64	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
46.19.86.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	64
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
99.8.13.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
100.100.1.104		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
45.50.179.51		147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
70.75.131.84	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.78.44	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
91.228.127.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
179.218.118.106	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
81.218.235.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
199.83.71.22	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
175.144.167.215	Malaysia	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.182.55.98	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
24.254.141.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.148.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
74.88.173.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
134.196.163.223	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
8.37.70.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.142.231.174	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
98.169.227.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.116.206.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
110.168.229.93	Thailand	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
99.8.13.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.142.231.174	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
220.181.108.163	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.204	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
50.116.28.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.75.76.6	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
207.46.13.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.121.192	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.216	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

10-31-2015-05:04:00 to 10-31-2015-06:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.122	Block	30
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	30
66.249.78.128	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	15
74.217.148.72	United States	147.237.72.166	aka.idf.il	Illegal HTTP Version chrome.exe HTTP/1.1	Block	15
66.249.75.76	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/14-he	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	15
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	15
66.249.69.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.6	Block	15
141.212.121.192	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	15
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	15
66.249.69.84	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.78.121	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on chinuch.aka.idf.il/404.htm	Block	15
66.249.67.243	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane/	Block	15
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1285-he/atal.aspx	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1146-he/chinuch.aspx	Block	15
175.144.167.215	Malaysia	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	15
74.217.148.72	United States	147.237.72.166	aka.idf.il	Abnormally Long Request request version	Block	15
66.249.69.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1274-he/atal.aspx	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/giyus/forum/asp/showforum.asp	None	15
178.47.203.181	Russian Federation	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1564-en/dover.aspx	Block	15
66.249.78.135	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/404.htm	Block	15
66.249.69.42	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/departmentslobby/departmentslobby.aspx	Block	15

10-31-2015-05:04:00 to 10-31-2015-06:04:00