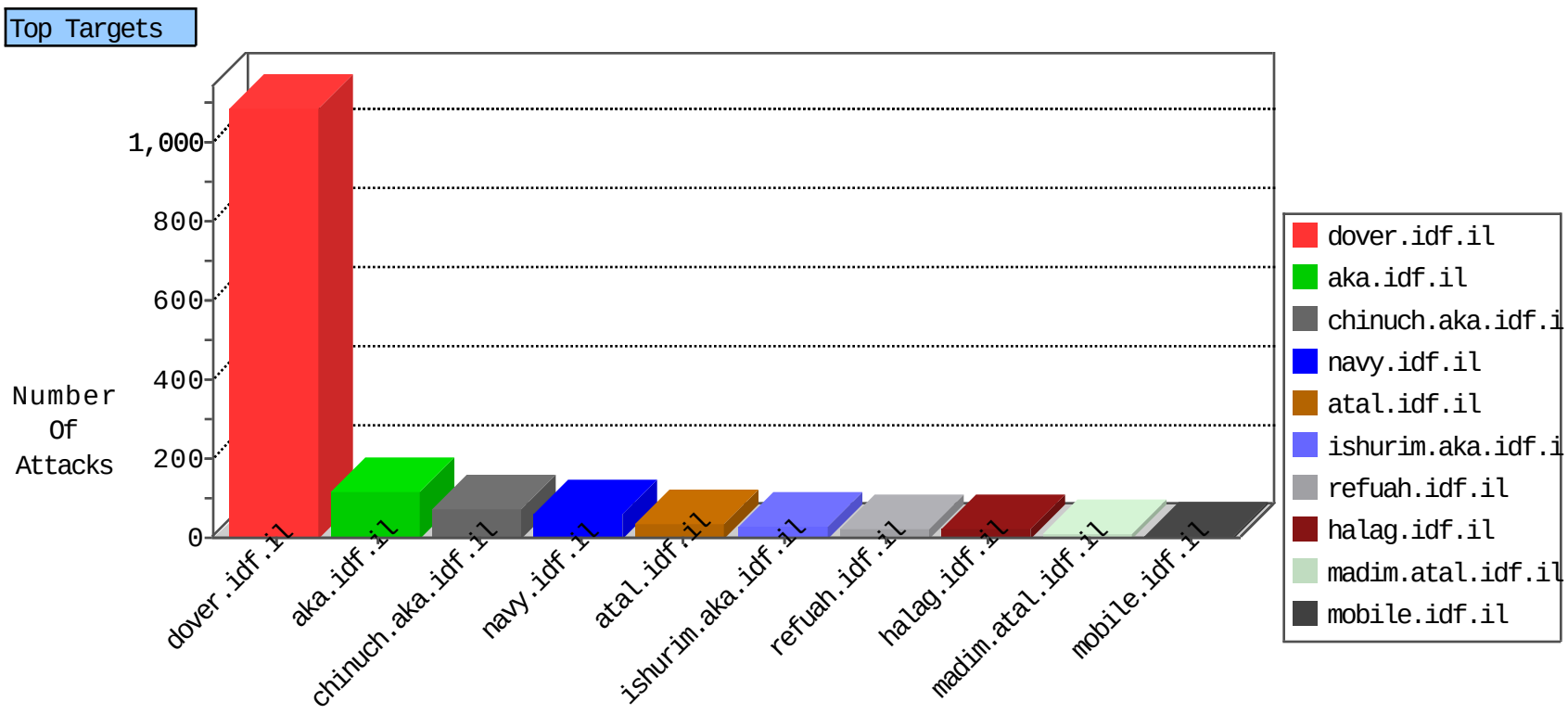
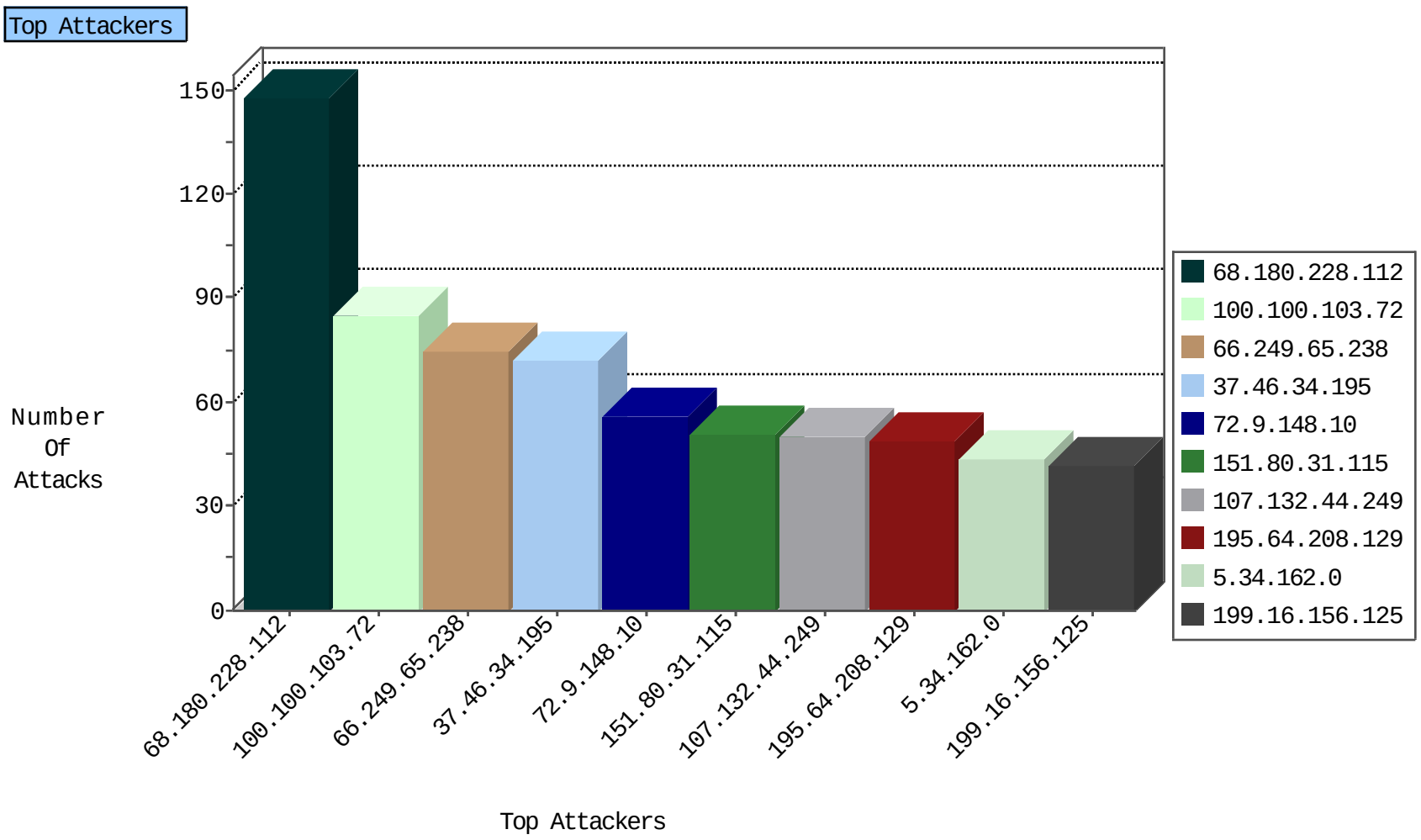
10-24-2015-07:04:03 to 10-24-2015-08:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-24-2015-07:04:03 to 10-24-2015-08:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.160.218.141	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	37
89.138.241.183	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.228.101.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
45.32.68.116		147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1

10-24-2015-07:04:03 to 10-24-2015-08:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.225.171.61	Iran, Islamic Republic of	147.237.77.234	halag.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	19
194.225.171.61	Iran, Islamic Republic of	147.237.77.234	halag.idf.i	0932: HTTP: Shell Command Execution (bash)	Block	1

10-24-2015-07:04:03 to 10-24-2015-08:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
104.156.251.119	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
104.156.251.119	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
88.241.169.30	147.237.76.30	Turkey	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.205.176.50	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
183.80.132.23	147.237.72.167	Vietnam	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
183.80.132.23	147.237.72.14	Vietnam	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
117.175.213.2	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.156.251.119	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential SSH Scan	1
104.156.251.119	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
46.151.52.8	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
183.80.132.23	147.237.72.217	Vietnam	e.idf.il	ET SCAN Potential SSH Scan	1
183.80.132.23	147.237.72.156	Vietnam	aman.idf.il	ET SCAN Potential SSH Scan	1
119.90.139.50	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1

10-24-2015-07:04:03 to 10-24-2015-08:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.46.34.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
107.132.44.249	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
195.64.208.129	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
5.34.162.0	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
100.100.103.72		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	44
109.160.134.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
84.228.110.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
78.53.233.229	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
46.19.86.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
100.100.103.72		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
37.54.255.16	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
192.114.185.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.103.72		147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
65.55.210.2	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
78.53.233.229	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.160.218.141	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.65.168.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
100.100.103.72		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	7
40.77.167.36	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.142.108.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.228.101.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.177.108.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.138	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.90.106	Israel	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
157.55.39.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
131.253.25.177	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.67.27	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.67.34	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
58.174.164.9	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.65.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.138	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.121.26.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
40.77.167.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.237.154.221	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

10-24-2015-07:04:03 to 10-24-2015-08:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.228.112	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	140
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	56
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/17418.jpg	Block	28
199.16.156.126	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/8/size220x0/17418.jpg	Block	28
40.77.167.42	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	28
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
40.77.167.43	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	28
40.77.167.44	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	14
157.55.39.94	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/	Block	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	14
2.54.20.144	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	14
81.209.177.189	Europe	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
46.19.86.209	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb13580537 in www.aka.idf.il/main/sachar/payslips.aspx	None	14
188.165.15.177	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	14
2.54.56.249	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	14
130.185.139.213	Denmark	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	14
66.249.64.249	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
199.16.156.124	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/8/size220x0/17418.jpg	Block	14
66.249.79.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	14
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/17401.jpg	Block	14
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/mainfs.asp	Block	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14

10-24-2015-07:04:03 to 10-24-2015-08:04:03