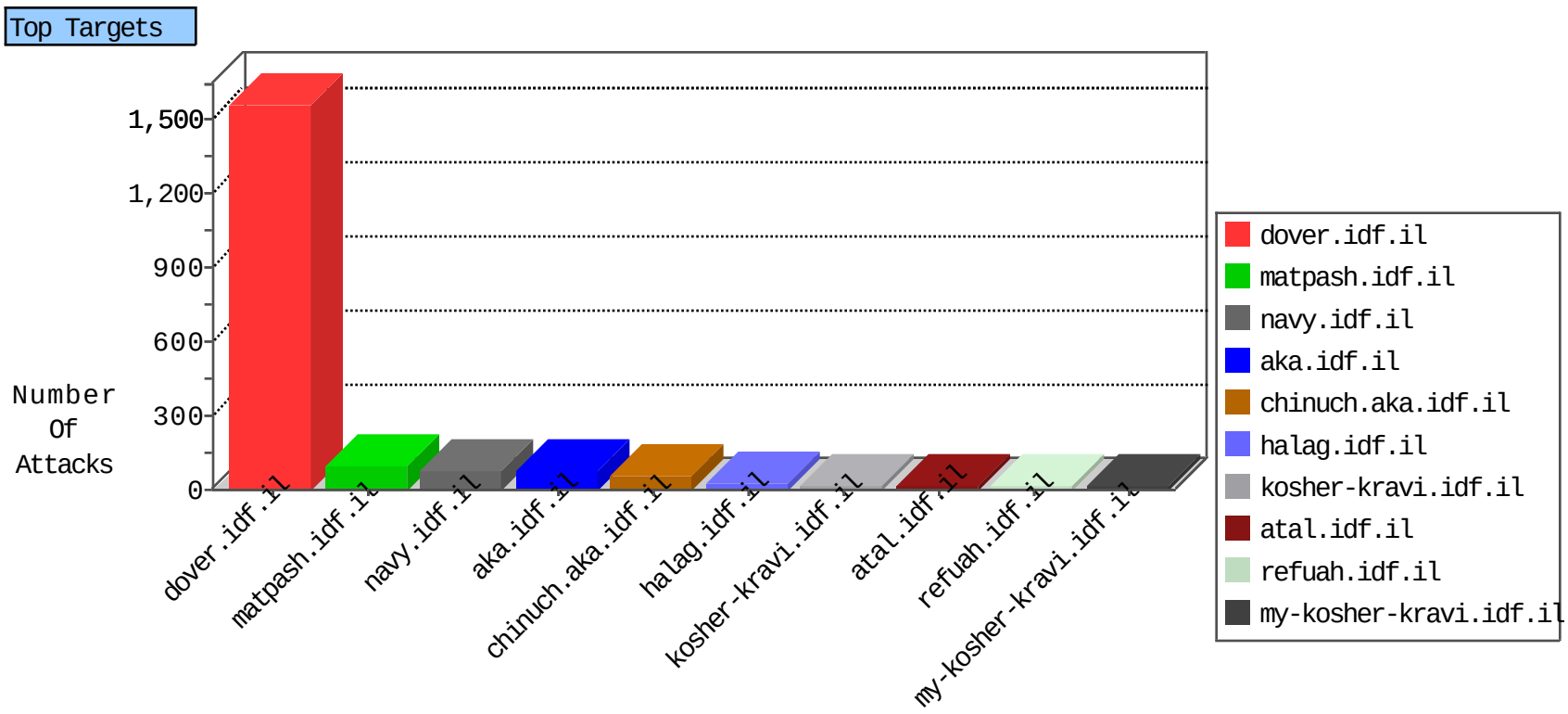
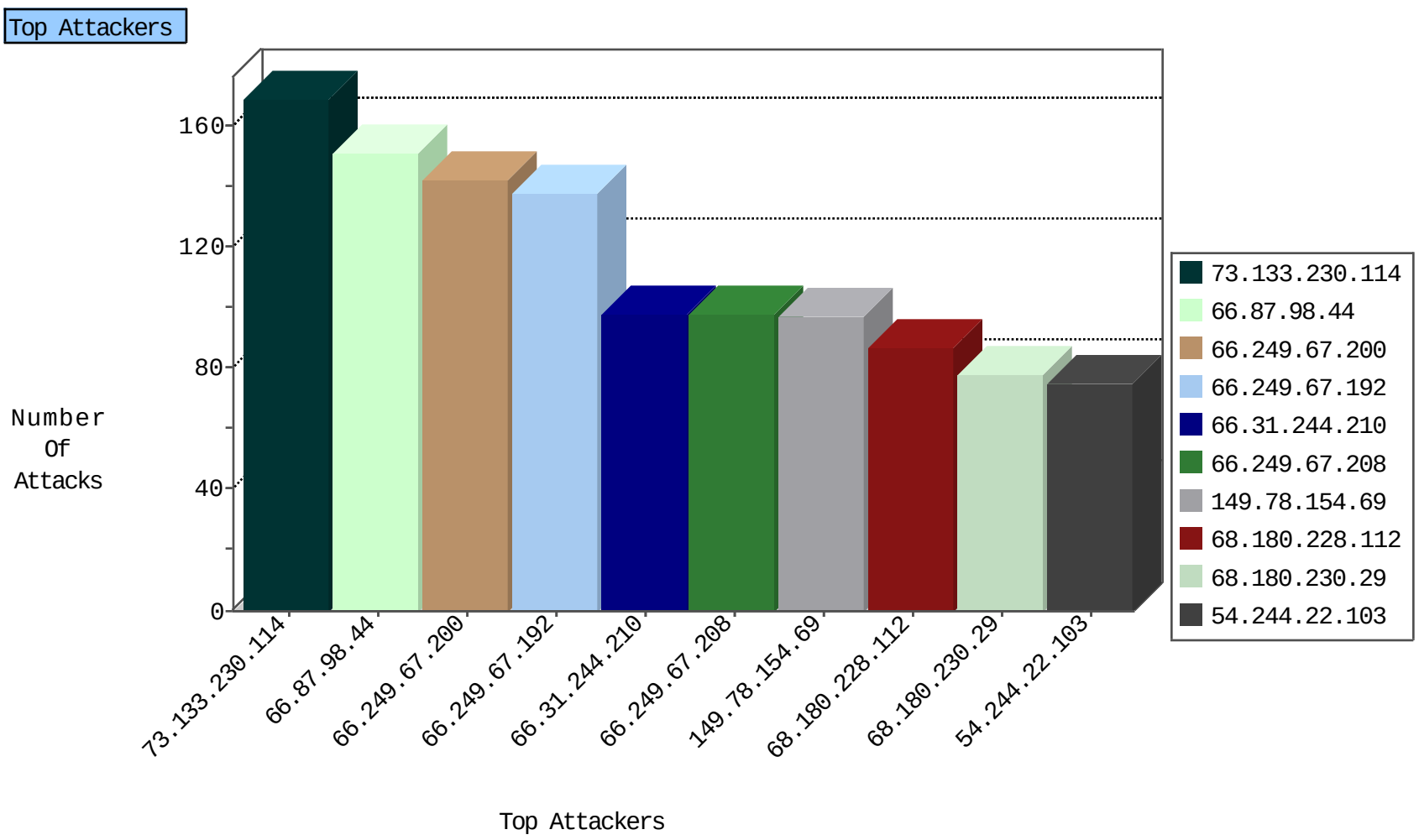
10-21-2015-04:04:05 to 10-21-2015-05:04:05

IDF Under Attack Daily Report





10-21-2015-04:04:05 to 10-21-2015-05:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
93.174.93.146	Netherlands	147.237.0.15	kosher-kravi.idf.il	Invalid TCP Flags	drop	1
89.248.172.98	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.146	Netherlands	147.237.76.197	e.himush.idf.il	Invalid TCP Flags	drop	1
89.248.172.98	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.100	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

10-21-2015-04:04:05 to 10-21-2015-05:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-21-2015-04:04:05 to 10-21-2015-05:04:05

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	3
174.128.228.82	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
223.4.210.53	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
188.53.142.211	147.237.77.121	Saudi Arabia	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
174.128.228.82	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
93.174.89.142	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
223.4.210.53	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
188.53.142.211	147.237.77.121	Saudi Arabia	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
188.53.142.211	147.237.77.121	Saudi Arabia	e.navy.idf.il	ET SCAN NMAP -f -sS	1
174.128.228.82	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential SSH Scan	1
128.199.95.16	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
223.4.210.53	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

10-21-2015-04:04:05 to 10-21-2015-05:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
73.133.230.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	169
66.87.98.44	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	151
66.31.244.210	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	97
84.111.62.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
98.211.110.170	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.102.8.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
113.159.159.59	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.102.8.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
108.18.122.45	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.244.22.103	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.67.200	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
199.30.16.171	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
52.16.5.197	United States	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	16
66.249.67.192	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
37.26.149.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	14
67.81.243.232	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
2.54.13.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
186.210.226.75	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
69.113.122.235	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
157.55.39.84	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
73.199.196.151	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.102.8.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
104.244.79.199		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.130.217.200	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	7
66.102.8.178	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.8.168	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
78.53.241.213	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
64.246.165.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.140.188.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
189.122.8.88	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
24.52.215.101	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
178.255.215.87	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

10-21-2015-04:04:05 to 10-21-2015-05:04:05

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	Distributed Suspicious Response Code	Block	78
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2110-he/cogat.aspx	Block	78
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.200	Block	65
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.192	Block	52
66.249.67.208	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.208	Block	52
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	52
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	39
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
66.249.67.208	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	26
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	26
66.249.81.137	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/1746-he/lifestyle.aspx	Block	13
77.237.138.51	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	13
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	13
61.135.190.197	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	13
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	13
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
66.249.67.208	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	13
64.246.165.200	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	13
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9236-he/refuah.aspx	Block	13
157.55.39.134	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/70259.jpg	Block	13
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	13
207.46.13.130	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	13
207.46.13.141	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	13

10-21-2015-04:04:05 to 10-21-2015-05:04:05