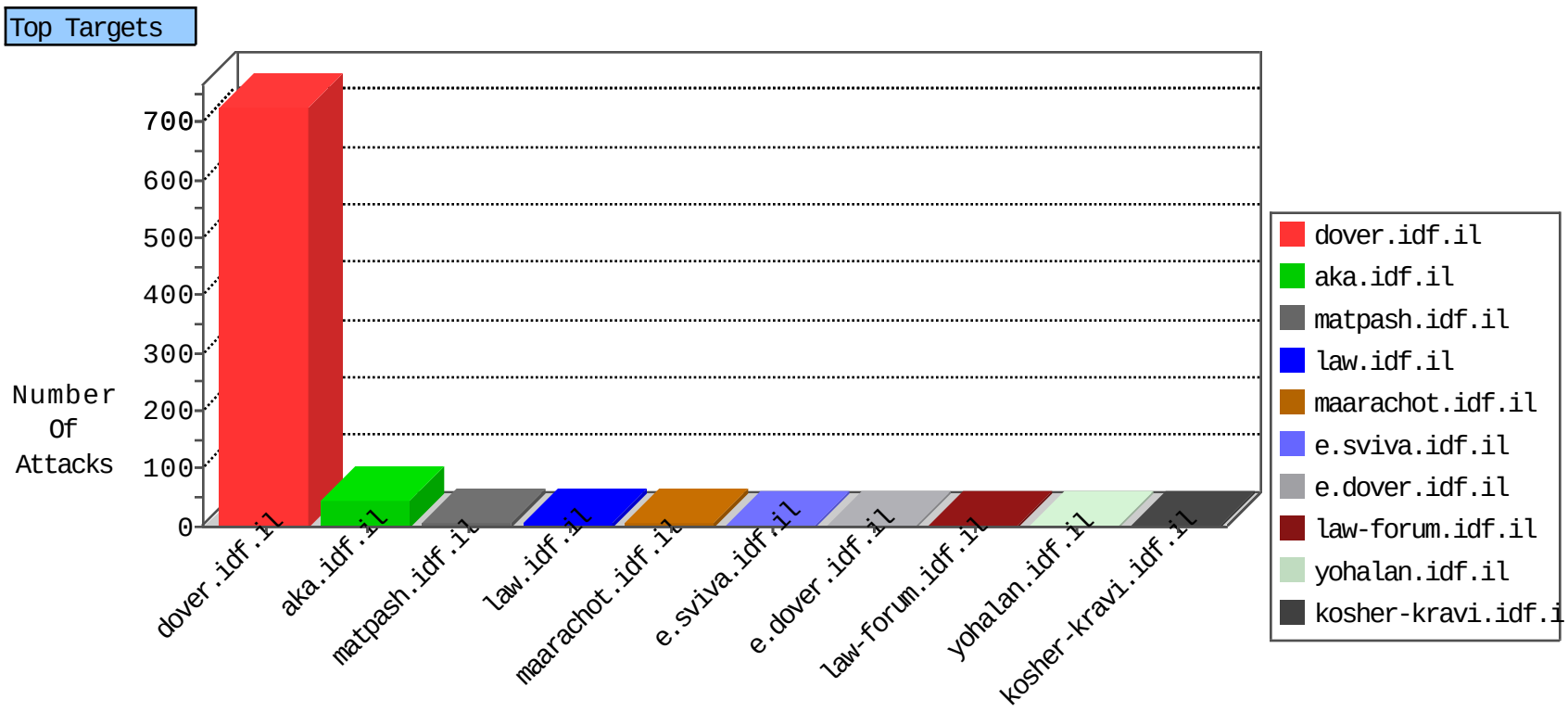
11-21-2015-03:04:05 to 11-21-2015-04:04:05

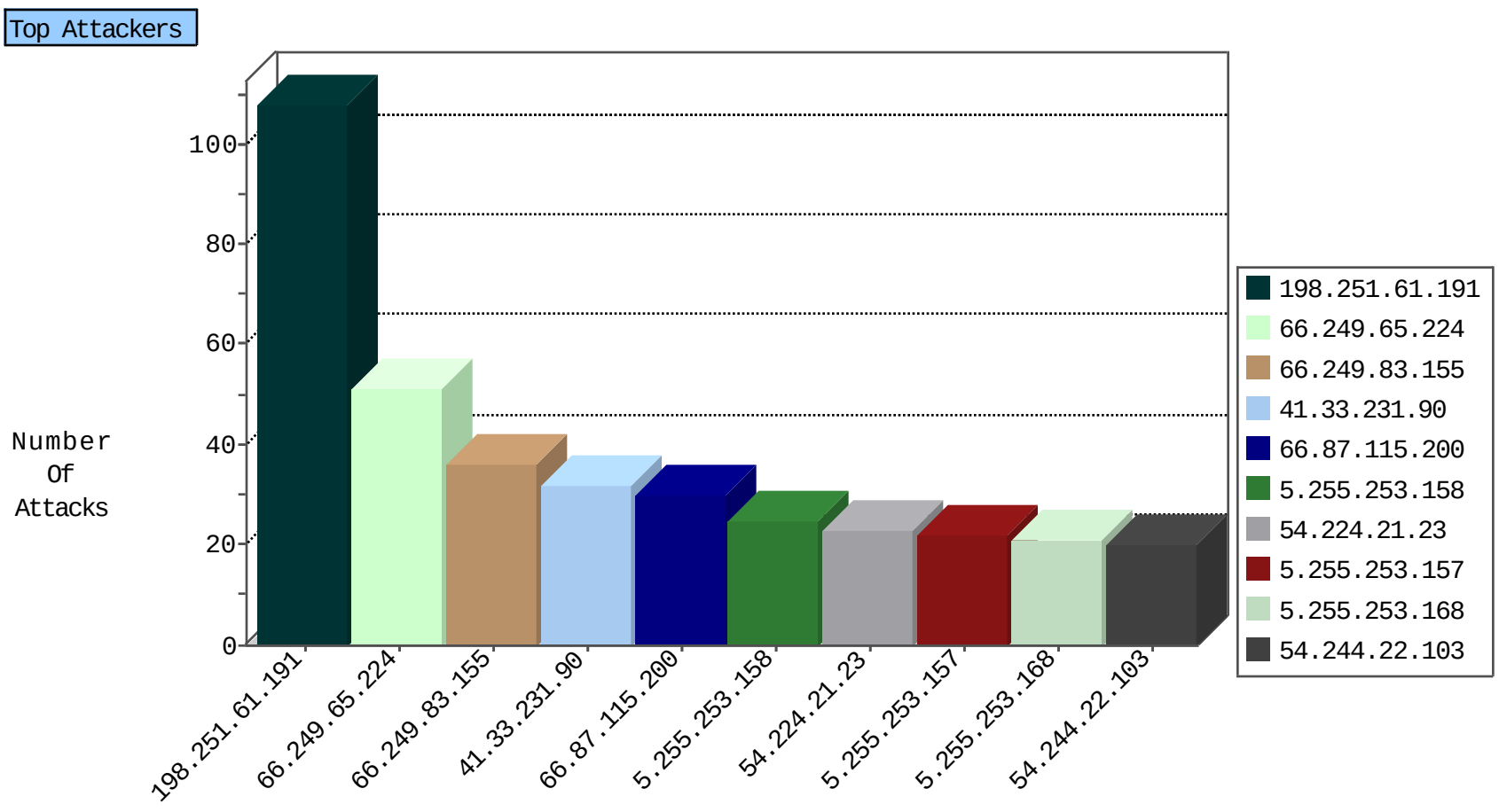
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-21-2015-03:04:05 to 11-21-2015-04:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.224.21.23	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1119
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	40
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
64.246.165.160	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	drop	1
104.192.0.226	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

11-21-2015-03:04:05 to 11-21-2015-04:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-21-2015-03:04:05 to 11-21-2015-04:04:05

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
66.249.67.67	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
5.28.156.96	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.65.224	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
42.112.36.35	147.237.76.196	Vietnam	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
42.112.36.35	147.237.76.196	Vietnam	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
184.172.196.106	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.151.55.35	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
42.112.36.35	147.237.76.196	Vietnam	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
120.59.178.93	147.237.77.216	India	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

11-21-2015-03:04:05 to 11-21-2015-04:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
198.251.61.191	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
66.249.83.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
66.87.115.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
5.255.253.158	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
37.188.230.47	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
107.161.181.105	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.249.83.158	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.83.161	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
108.59.253.71	United States	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
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
5.255.253.170	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
141.8.142.11	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
173.252.89.55	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
199.16.156.125	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
199.16.156.126	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
107.178.194.83	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
165.228.54.133	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
96.28.106.48	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.91.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.91.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
199.16.156.124	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
37.18.51.226	Russian Federation	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
65.19.138.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
173.252.89.58	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
166.137.118.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
173.252.89.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.209.60.63	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.67.122	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.254.158.75	Latvia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.52.171.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
64.246.165.160	United States	147.237.0.15	kosher-kravi.idf.il	Header Rejection	header rejection pattern found in request	monitor	3
107.178.194.79	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	19
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	5
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	4
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
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	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.231	Block	2
5.29.254.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.5.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
99.25.154.228	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
66.249.67.132	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/reserve	Block	1
212.143.91.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
157.55.39.132	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyuis	Block	1
194.90.116.95	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
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	1
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	1
216.55.143.94	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name Mozilla/5.0 (compatible; spider/2.0; +http	Block	1
157.55.39.145	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
77.237.138.51	Czech Republic	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	1
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	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
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	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
157.55.39.169	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/edim/fund/Ã£â€”Ã¢â‚¬Ëœâ€”Ã¢â‚¬Â?Ã£â€”Ã¢Â§Ã£â€”Ã¥Â¾Ã£â€”Ã¢â‚¬Â?	Block	1
79.179.142.147	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.189	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
109.65.144.46	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
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	1
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
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	1
141.212.122.160	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
68.180.231.40	United States	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.law.idf.il/163-6639-he/patzar.aspx	Block	1
31.154.94.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.i	Unknown Parameter l in www.chinuch.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1