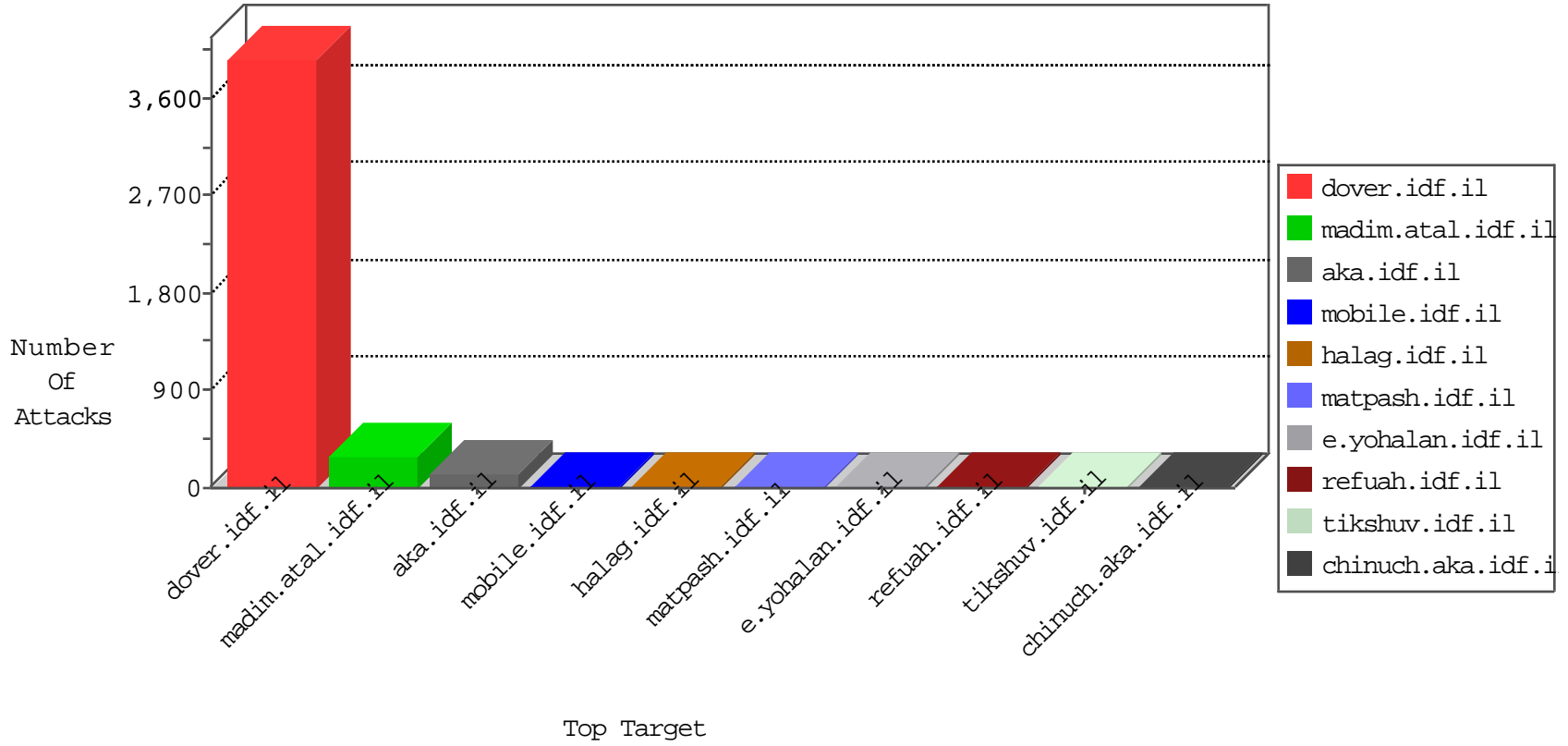


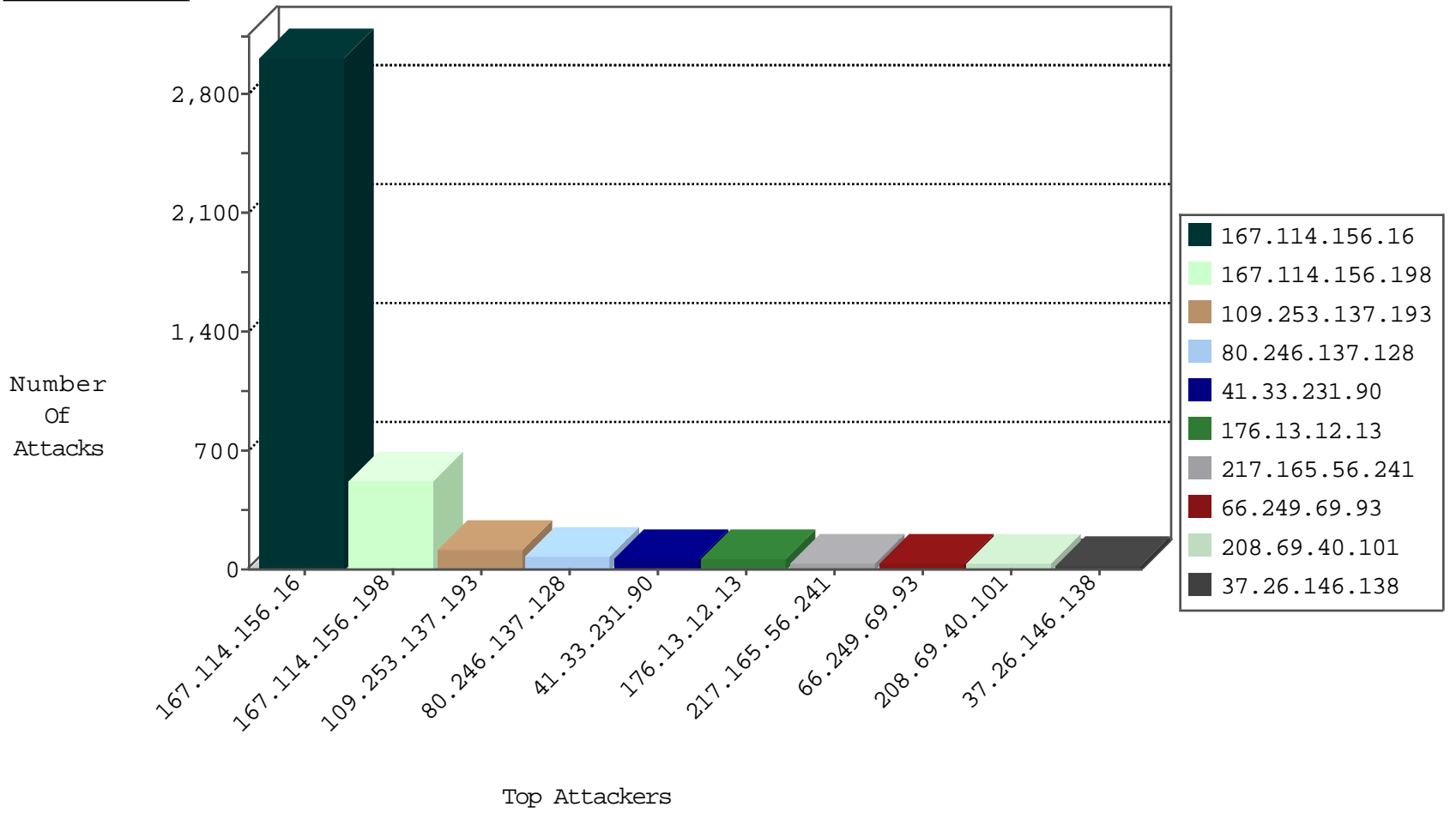
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1680
188.138.1.218	Germany	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
218.200.212.213	China	147.237.0.200	m4u.idf.il	Frk_Purple_Con_Limit_Http	drop	1

04-21-2016-07:04:00 to 04-21-2016-08:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	1

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	3
67.130.39.67	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
109.235.254.181	147.237.76.147	Turkey	chinuch.aka.idf.i	ET SCAN NMAP -sS window 2048	1
91.187.18.47	147.237.0.35	Belarus	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
67.130.39.67	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
109.235.254.181	147.237.76.147	Turkey	chinuch.aka.idf.i	ET SCAN NMAP -sS window 3072	1
109.235.254.181	147.237.76.147	Turkey	chinuch.aka.idf.i	ET SCAN NMAP -f -sS	1
67.130.39.67	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1892
167.114.156.198	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	510
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
217.165.56.241	United Arab Emirates	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
37.26.146.138	Israel	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	21
5.254.65.232	Turkey	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	19
207.241.229.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	19
188.73.128.158	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
40.77.167.25	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
95.187.16.53	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.149.207	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	6
176.13.15.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.22.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	5
17.138.55.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.120.98.114	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.26.147.157	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
66.249.93.15	Israel	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.179.90.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.93.18	Europe	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.254.65.232	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.167.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
64.246.165.190	United States	147.237.77.176	matpash.idf.il	Header Rejection	header rejection pattern found in request	monitor	4
95.35.188.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.90.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.67.62.51	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.129.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.79.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.207	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.137.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
80.246.137.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	68
176.13.12.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
37.26.149.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
17.138.55.96	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.55.96	Block	11
109.186.56.14	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.186.56.14	Block	11
109.186.56.14	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	10
2.53.14.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
84.111.122.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	6
109.186.173.101	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.186.173.101	Block	4
46.19.85.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
82.166.53.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.144.60.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
216.218.206.67	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/searchback.png	Block	1
109.253.222.6	Israel	147.237.77.216	dover.idf.il	Redundant HTTP Headers Referer	Block	1
81.218.37.2	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/topcap.gif	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.69.34	Block	1
80.246.133.37	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz/res#012 ources/images/innerpage/goback.gif	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17770-	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/ 5	Block	1
207.46.13.56	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
80.246.133.37	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 80.246.133.37	Block	1
167.114.156.198	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.75.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/smalim.aspx	Block	1
207.46.13.115	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/home/default.asp@catid=43314	Block	1
109.186.173.101	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
80.246.136.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
46.19.85.50	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
167.114.156.198	Canada	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 167.114.156.198	Block	1
109.64.9.27	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
212.235.103.219	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8818-he/refuah.aspx	Block	1
167.114.156.198	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
73.25.158.80	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1