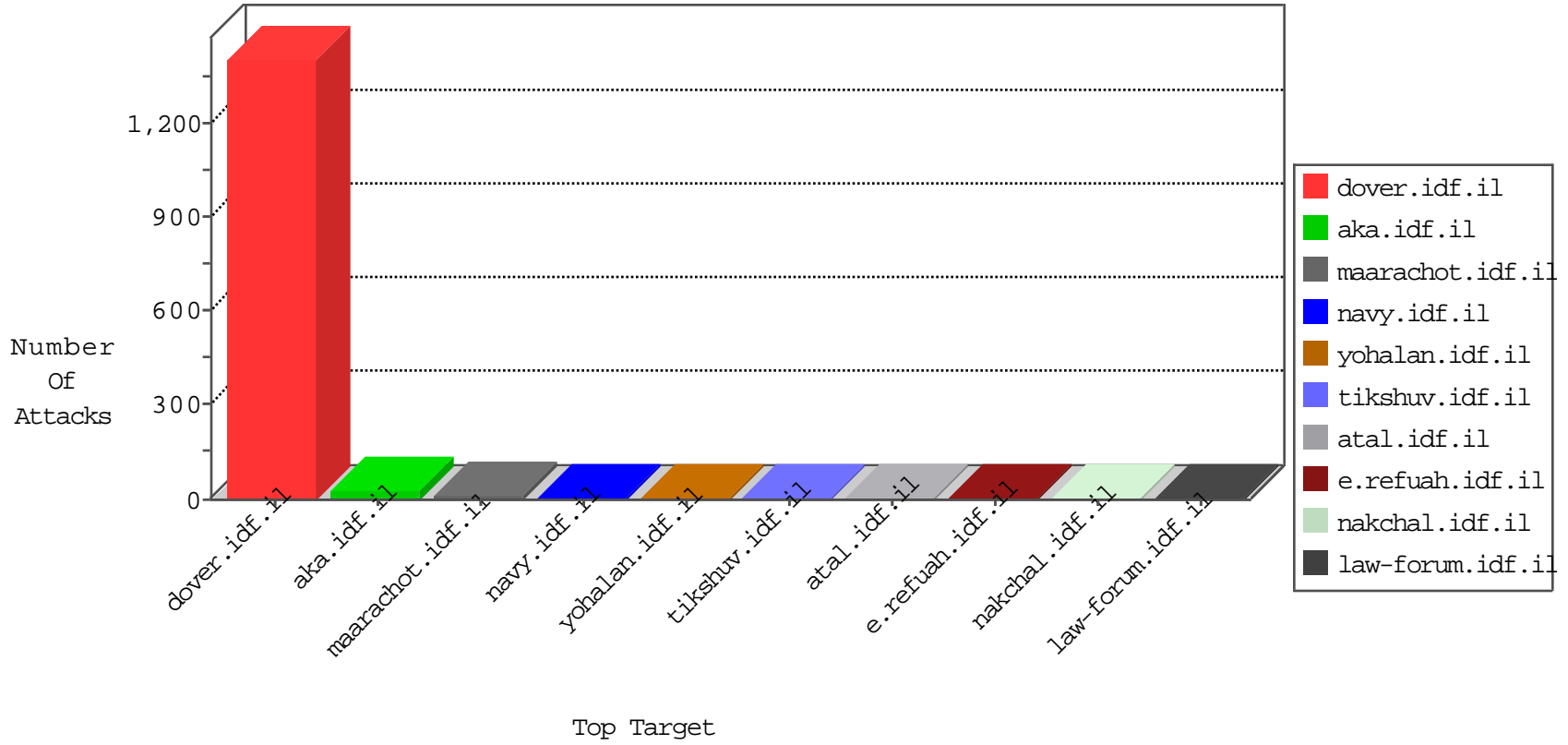


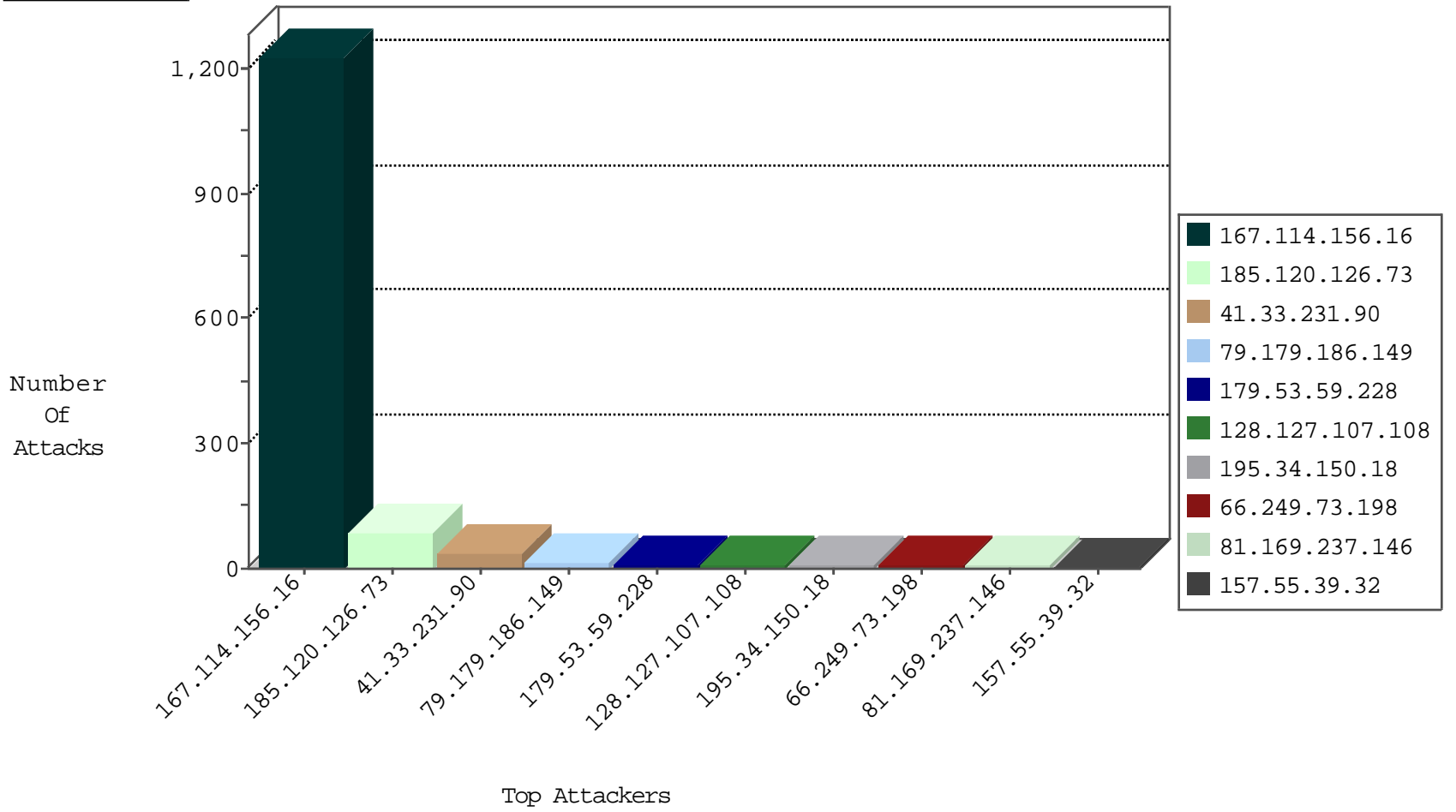
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6296
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3051
157.55.39.32	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
61.160.247.202	China	147.237.76.34	yohalan.idf.il	JLM_Under_Attack_Con_Http	drop	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
208.67.1.66	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
141.212.122.198	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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
66.249.73.206	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
190.249.184.162	147.237.77.19	Colombia	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
187.160.152.143	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
179.33.34.162	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
167.88.9.227	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.162.131	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.77.233	Germany	atal.idf.il	ET SCAN Potential SSH Scan	1
190.249.184.162	147.237.77.19	Colombia	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
185.100.85.148	147.237.72.167		ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.20.29	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.228.207.18	147.237.76.44	Germany	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	27
79.179.186.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
179.53.59.228	Dominican Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.28.172.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.45.254.226	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
98.252.51.195	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.179.186.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
128.127.107.108	Netherlands	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
66.225.122.26	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	2
157.55.39.15	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
179.53.59.228	Dominican Republic	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	2
157.55.39.75	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.212.122.149	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.174.93.203	Netherlands	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
179.53.59.228	Dominican Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
151.80.164.147	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.121.172	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.114	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.127.107.108	Netherlands	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
184.105.139.115	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
54.183.120.101	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.150	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.127.107.108	Netherlands	147.237.76.147	chimuch.aka.idf.il	drop	SAM rule	drop	1
94.230.86.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
179.53.59.228	Dominican Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.22	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.121.173	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.120	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.127.107.108	Netherlands	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
184.105.247.204	United States	147.237.0.35	akaws.idf.il	drop		drop	1
81.169.237.146	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
54.183.120.101	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.156	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.127.107.108	Netherlands	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
179.53.59.228	Dominican Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
157.55.39.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
8.37.226.2	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.121.175	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
128.127.107.108	Netherlands	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
184.105.247.248	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.70.90	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/dover.aspx&usg=alkjrhgmz1w1lc6gopjwihsdssrbfsaq	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.21	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
184.105.247.196	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
50.153.189.113	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.179.186.149	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.179.186.149 (Open Mode)	None	1
66.249.66.27	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.230.57	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
54.183.120.101	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
79.179.186.149	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
54.183.120.101	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
157.55.39.75	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.40.129.123	Block	1
66.249.64.193	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1774	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-14840-en/kkkkkkk=2237975bkkkkkkk_2237975b	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1