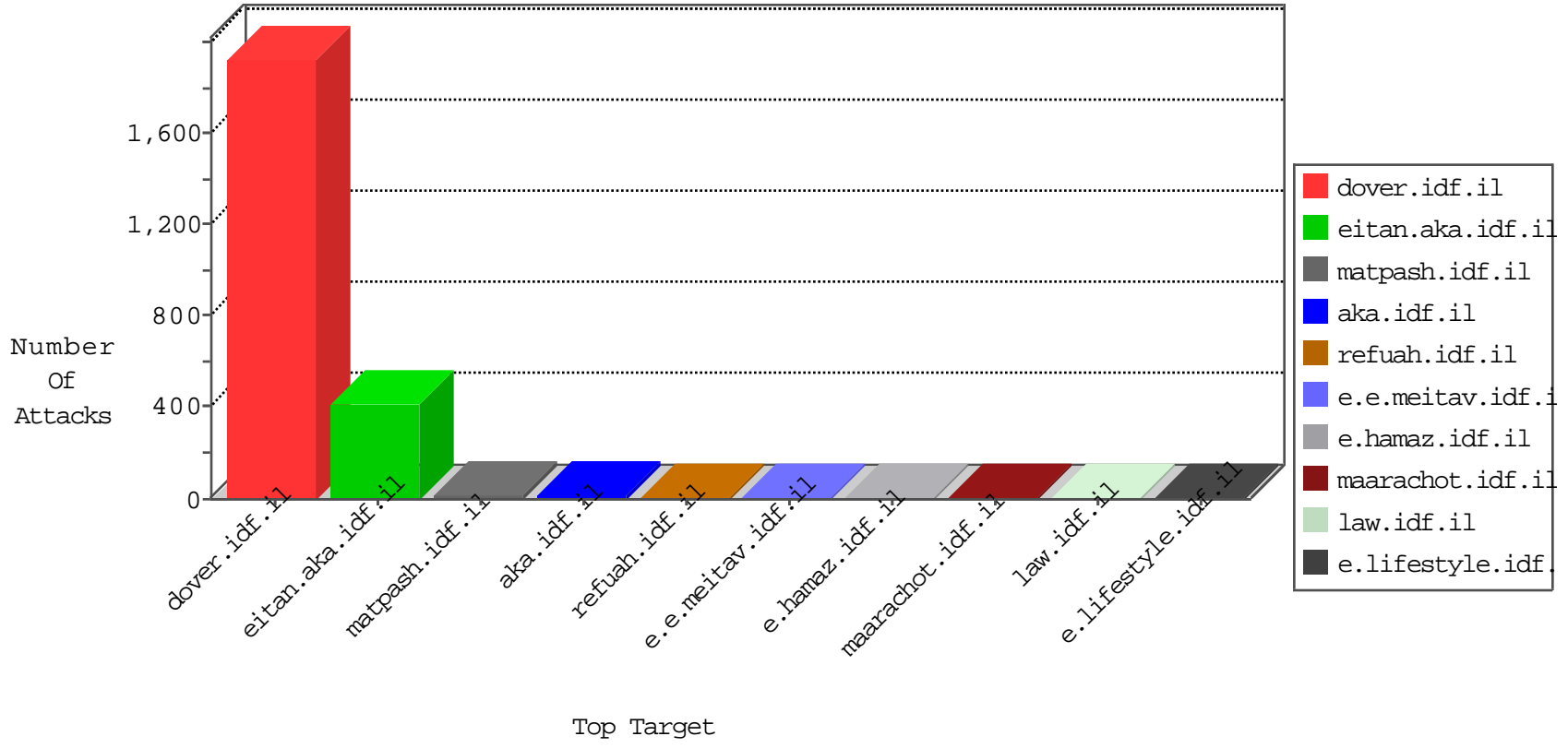


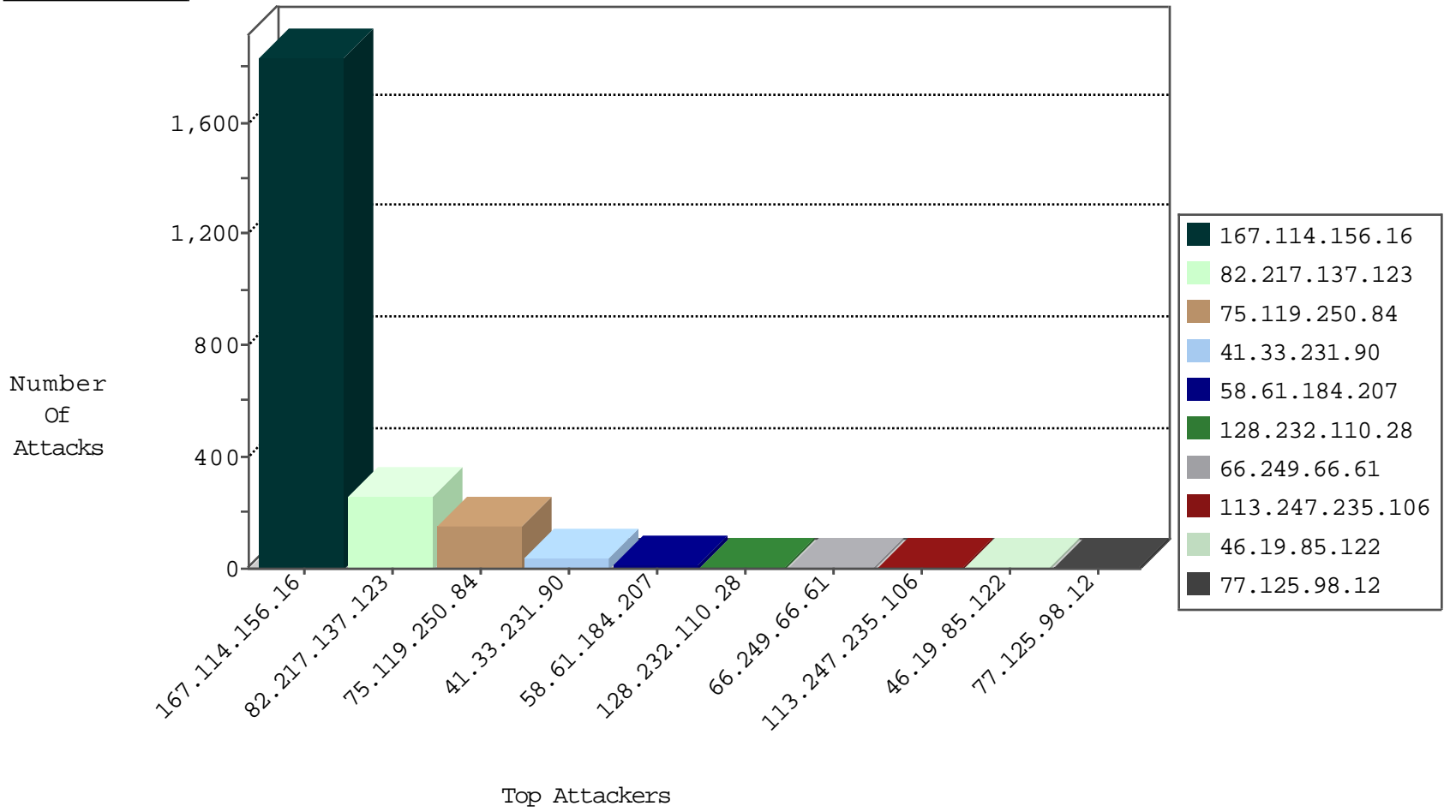
IDF Under Attack Daily Report



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	3172
36.57.254.6	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
36.57.254.6	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.25	Israel	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	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	4
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
50.204.188.142	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
201.175.113.79	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.82.106.200	147.237.76.201	India	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
159.122.238.155	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
94.102.48.195	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.66.181	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.77.54.132	147.237.8.27	Korea, Republic of	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
201.175.113.79	147.237.77.233	Mexico	atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
201.173.59.246	147.237.0.17	Mexico	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.82.106.200	147.237.76.201	India	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
159.122.238.155	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
104.219.238.10	147.237.77.179		e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
84.117.113.152	147.237.77.227	Romania	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.217.137.123	Netherlands	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	152
75.119.250.84	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
46.19.85.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.125.98.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
40.77.167.7	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
113.247.235.106	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
133.130.54.151	Japan	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
128.232.110.28	United Kingdom	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
128.232.110.28	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
113.247.235.106	China	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	2
74.82.47.15	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.104	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.118	United States	147.237.8.24	e.lifestyle.idf	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.84	United States	147.237.76.199	e.nakchal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.155	United States	147.237.8.24	e.lifestyle.idf	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.55	United States	147.237.0.33	idf.il	drop		drop	1
216.218.206.118	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
31.210.186.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.120	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.153	United States	147.237.76.38	e.e.meitav.idf.	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
99.234.204.148	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.84	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.156	United States	147.237.8.24	e.lifestyle.idf	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.59	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
207.46.13.77	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.153	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.65.42.26	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.90	United States	147.237.76.38	e.e.meitav.idf.	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
210.48.190.30	New Zealand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.154	United States	147.237.76.38	e.e.meitav.idf.	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.90	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.154	United States	147.237.76.86	navy.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
75.119.250.84	Canada	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 75.119.250.84	Block	104
82.217.137.123	Netherlands	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	104
58.61.184.207	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 58.61.184.207	Block	6
45.55.41.246		147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 45.55.41.246	Block	3
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
58.61.184.207	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/contact.asp	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
75.119.250.84	Canada	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
58.61.184.207	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 58.61.184.207	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/media.asp	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.181	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
45.55.41.246		147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/shared/usercontrols/headerupper/	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 195.154.227.118	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
113.247.235.106	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/usercontrols/headerupper/	Block	1
66.249.75.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/9236.jpg	Block	1
66.249.66.31	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/elram	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
123.125.71.44	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 68.180.228.175	Block	1
58.61.184.207	China	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
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
213.152.173.135	Netherlands	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
157.55.39.194	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1