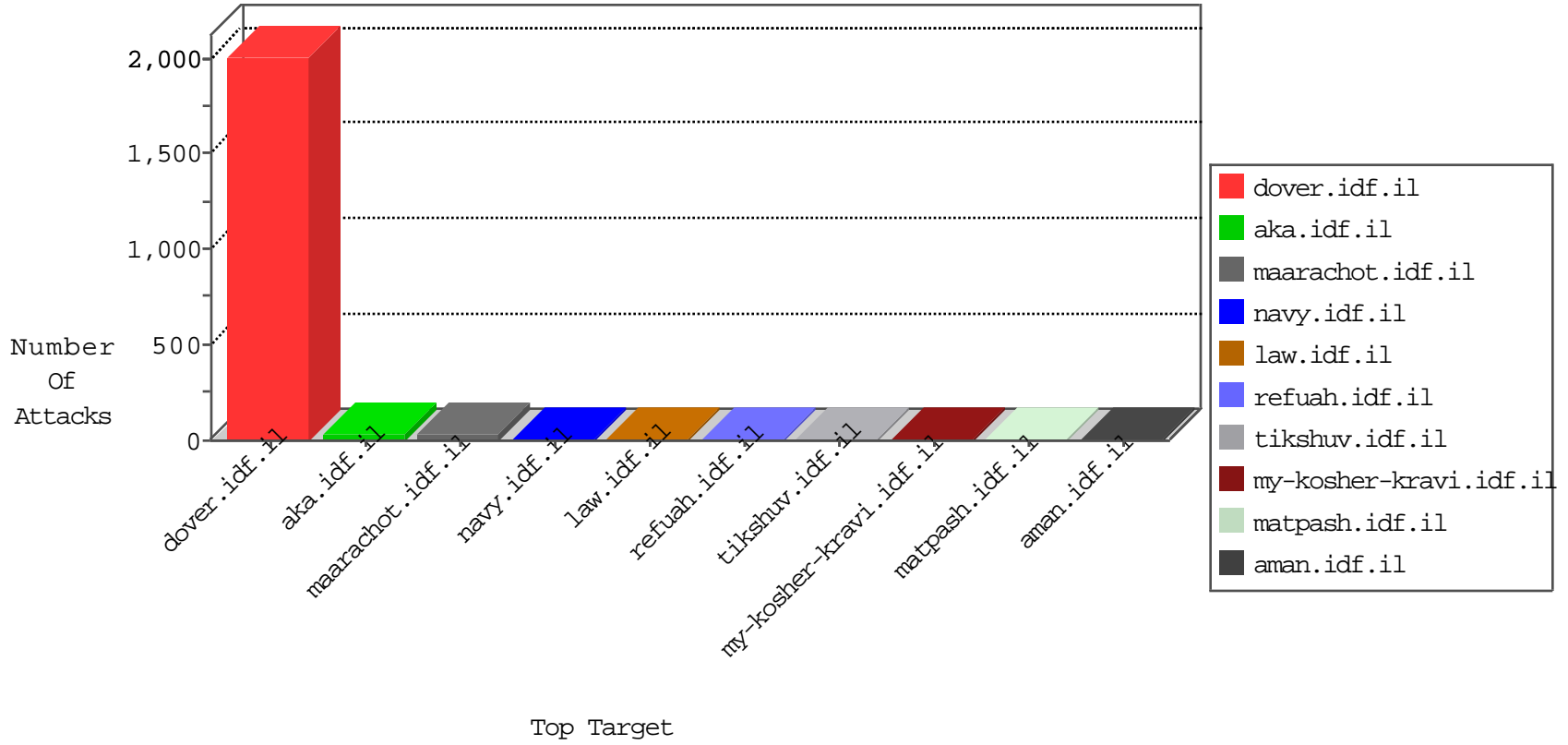


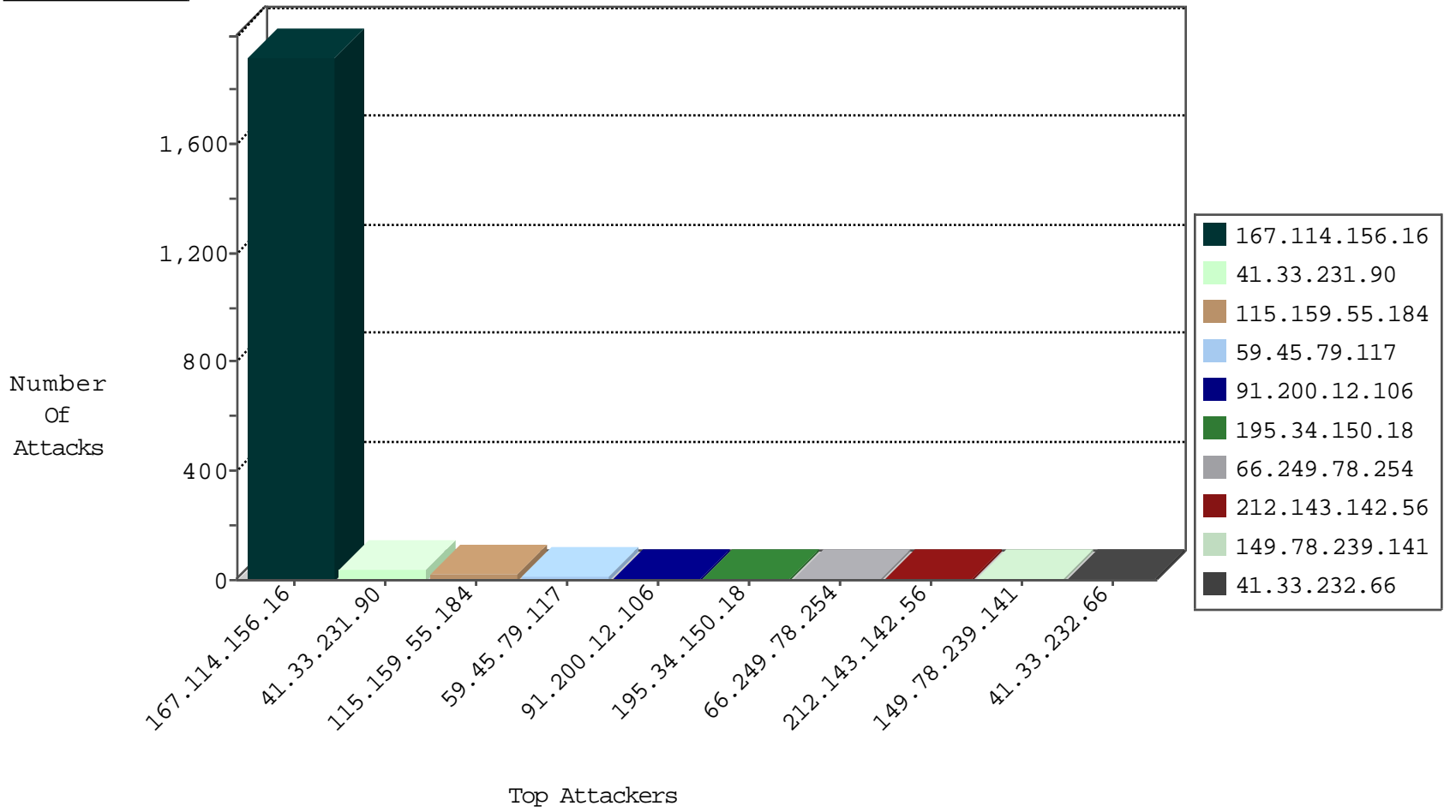
IDF Under Attack Daily Report



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	3125
95.24.16.130	Russian Federation	147.237.76.42	refuah.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	4
172.98.200.238	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 1024	1
125.78.177.98	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.192.0.226	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
201.166.231.2	147.237.0.33	Mexico	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
183.61.109.189	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
172.98.200.238	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 2048	1
172.98.200.238	147.237.77.234		halag.idf.il	ET SCAN NMAP -f -sS	1
125.65.165.215	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.61.109.189	147.237.0.16	China	my-kosher-kravi.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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
115.159.55.184	China	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	22
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
66.249.78.254	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.239.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.136	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.106	Ukraine	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
66.249.64.172	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
109.67.115.55	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
180.76.15.16	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
184.105.247.203	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
68.135.50.82	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.91	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.154.146.225	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
184.105.139.82	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.247.212	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.122	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.1	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.114	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.73	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
184.105.247.251	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
74.82.47.6	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
184.105.139.120	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
74.82.47.14	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
208.115.111.73	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
184.105.139.124	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
68.135.50.82	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
195.66.76.4	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	2
84.94.38.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for ww.aka.idf.il/main/giyus/authenticationsevice.aspx/getauthuser	Block	2
207.241.237.211	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/error.htm	Block	2
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
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	2
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
74.82.47.2	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.66.142	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list6.htm	Block	1
149.88.81.12	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
95.175.35.73	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/shared/usercontrols/headerupper	Block	1
66.249.79.228	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.79.228	Block	1
46.166.186.200	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
109.67.115.55	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkk=ad1f3caekkkkkk_ad1f3cae	Block	1
104.131.147.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/2974.jpg	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12801-h	Block	1
109.127.77.123	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
87.226.83.73	Latvia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
184.105.139.70	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	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
66.249.79.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3250.jpg	Block	1
109.201.135.58	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
87.226.83.73	Latvia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/headers/aboutsite.gif	Block	1
184.105.139.70	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
68.135.50.82	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.88.81.12	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 149.88.81.12 (sigalgs DoS Attack)	None	1
95.108.132.178	Russian Federation	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 95.108.132.178	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
199.30.24.213	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1