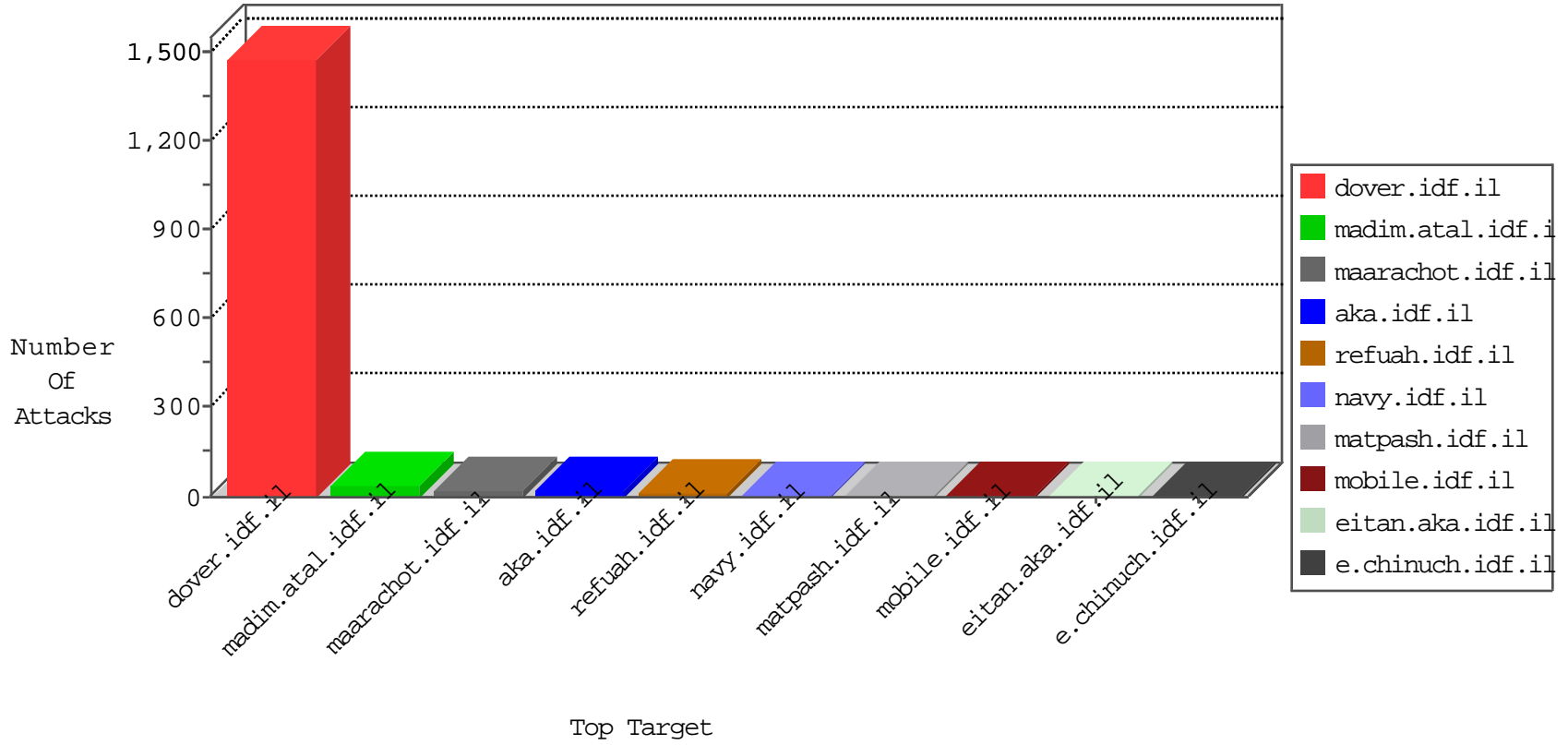


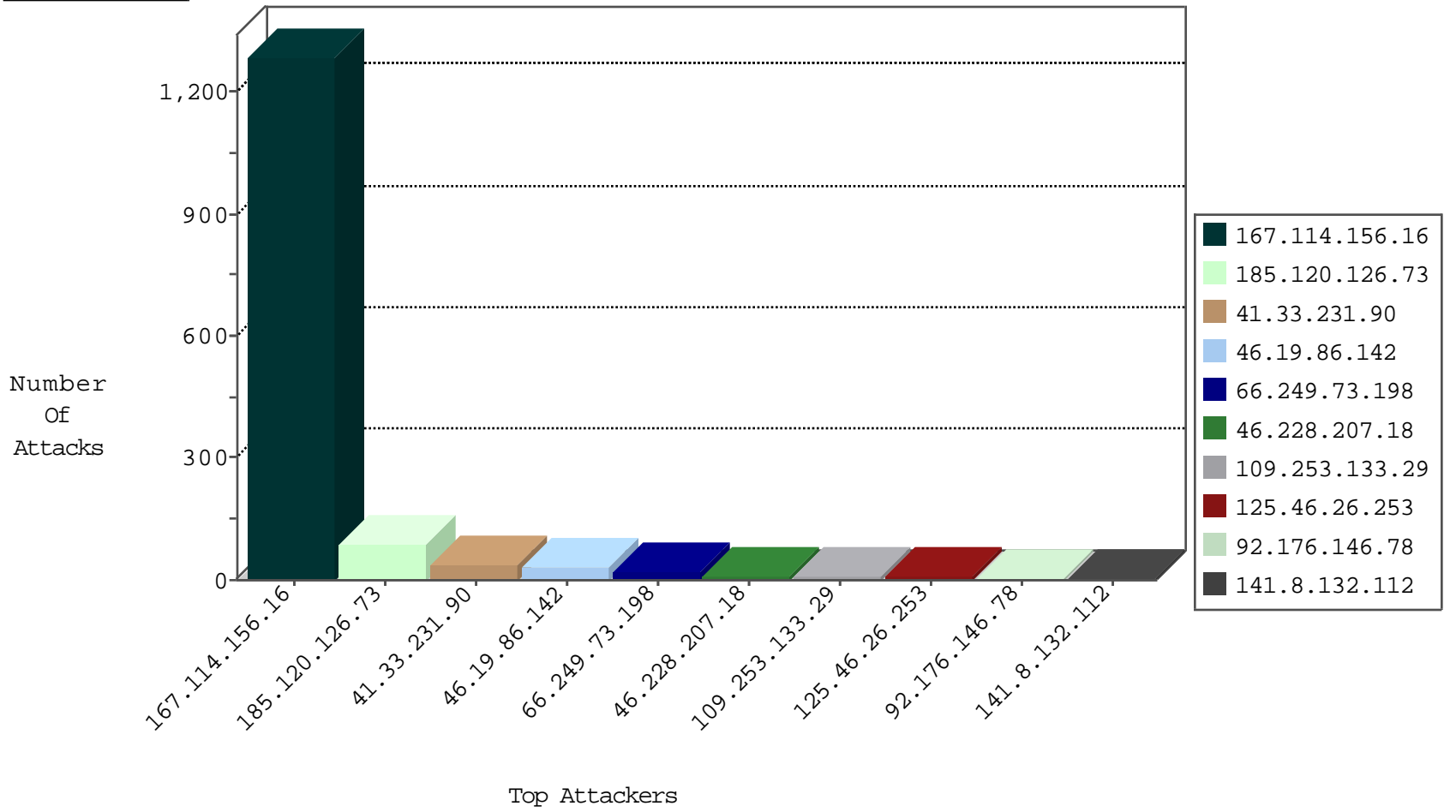
IDF Under Attack Daily Report



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	7155
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3165

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.240.213.93	United States	147.237.8.46	e.chinuch.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	2
83.161.67.152	Netherlands	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
106.120.201.115	147.237.0.200	China	m4u.idf.il	GPL SCAN nmap TCP	2
89.248.162.131	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.77.216	Germany	dover.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.76.39	Germany	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.72.14	Germany	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.0.33	Germany	idf.il	ET SCAN Potential SSH Scan	1
46.165.222.227	147.237.77.178	Germany	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
5.148.157.229	147.237.77.205	United Kingdom	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.162.131	147.237.76.148	Netherlands	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.248.146.42	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.202	Germany	e.halag.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.76.34	Germany	yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.0.35	Germany	akaws.idf.il	ET SCAN Potential SSH Scan	1
46.165.222.227	147.237.77.226	Germany	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.165.222.227	147.237.76.176	Germany	test.noore.idf.il	ET SCAN NMAP -sS window 1024	1
212.3.105.128	147.237.0.33	Ukraine	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	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	29
92.176.146.78	France	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	5
199.30.24.201	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
82.80.168.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	2
65.124.217.199	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
24.164.130.147	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
128.127.107.108	Netherlands	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
66.249.66.95	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
40.77.167.43	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
85.250.95.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
108.235.10.4	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.250.240.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
98.252.51.195	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	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
65.124.217.199	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
141.212.122.183	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.174	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.94	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.174.93.203	Netherlands	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.188	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
76.21.116.21	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.157	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.170	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.154.226.90	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
5.102.254.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
100.36.41.175	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.184	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.145	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.227	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.188	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
76.21.116.21	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.158	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.171	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.255.253.101	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
108.35.187.52	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
174.118.59.7	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.185	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
69.116.241.150	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
109.253.133.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
125.46.26.253	China	147.237.76.42	refuah.idf.il	PHP Attempt	Block	2
125.46.26.253	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/admin-ajax.php	Block	2
207.46.13.24	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
141.212.122.145	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
74.82.47.3	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
180.76.15.139	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
125.46.26.253	China	147.237.76.42	refuah.idf.il	Multiple Admin Blocking from 125.46.26.253	Block	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
141.212.122.145	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
79.179.186.149	Israel	147.237.76.39	mobile.meitav.idf.il	SSL Untraceable Connection - Open Mode	None	1
200.98.66.161	Brazil	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13437-he/dover.aspxx³Ö³Æ'Ö²Ä-Ö³æšÖ²ÄçÖ³æš Ö²Ä½³Ä³Ö³Æ'Ö²Ä-Ö³æšÖ²ÄçÖ³æšÖ²Ä½³Ä³Ö³Æ'Ö²Ä-Ö³æšÖ²ÄçÖ³æš Ö²Ä½³Ä³Æ	Block	1
148.251.21.227	Germany	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 148.251.21.227	Block	1
107.178.195.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
37.186.100.63	Armenia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
200.98.66.161	Brazil	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/images/xxu.php	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/sidebar/sidebar.js	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
148.251.21.227	Germany	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/320/patzar.aspx	Block	1
46.19.85.254	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	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
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
209.190.113.85	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/shared/usercontrols/headerupper/	Block	1
172.250.84.201	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
125.46.26.253	China	147.237.76.42	refuah.idf.il	Admin Blocking	Block	1