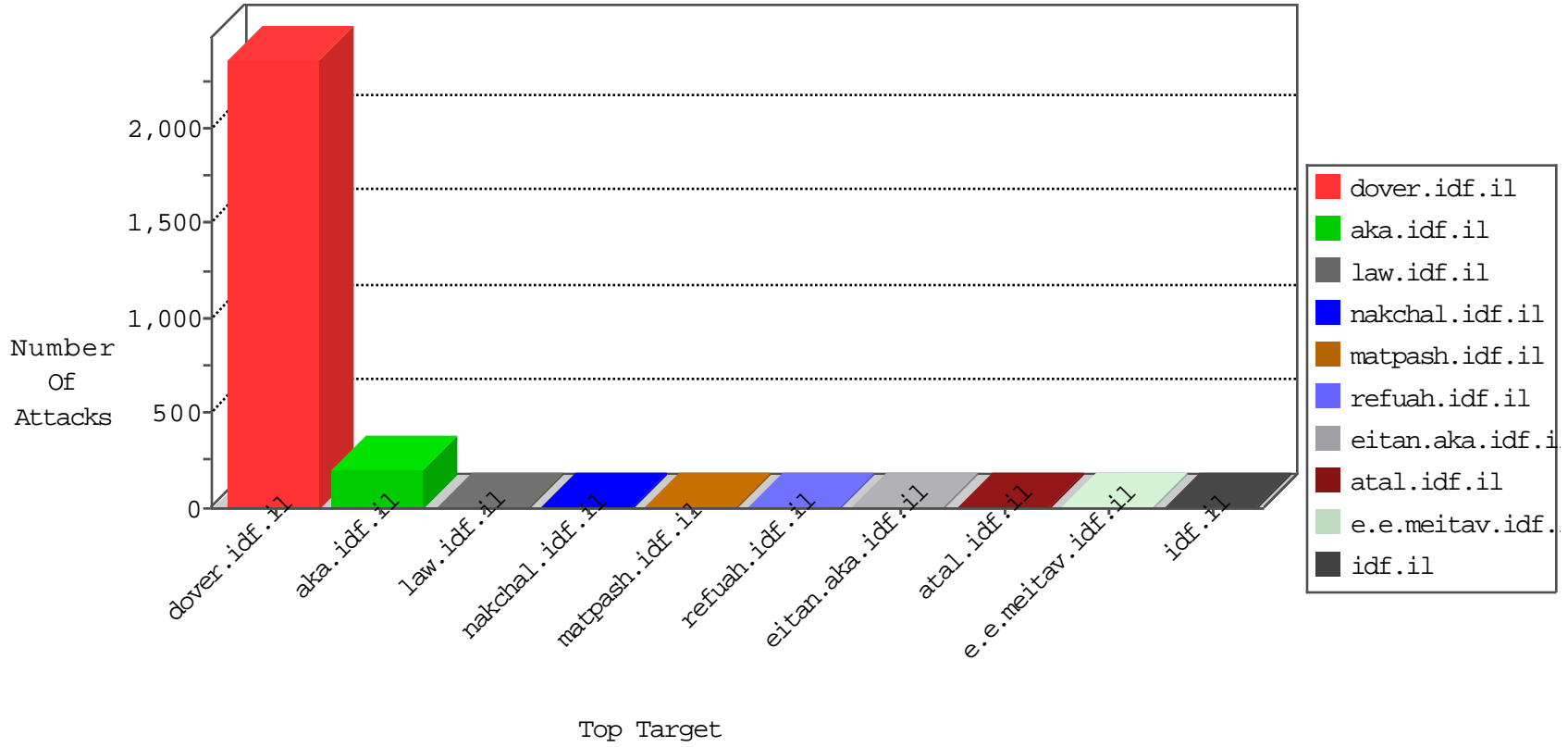




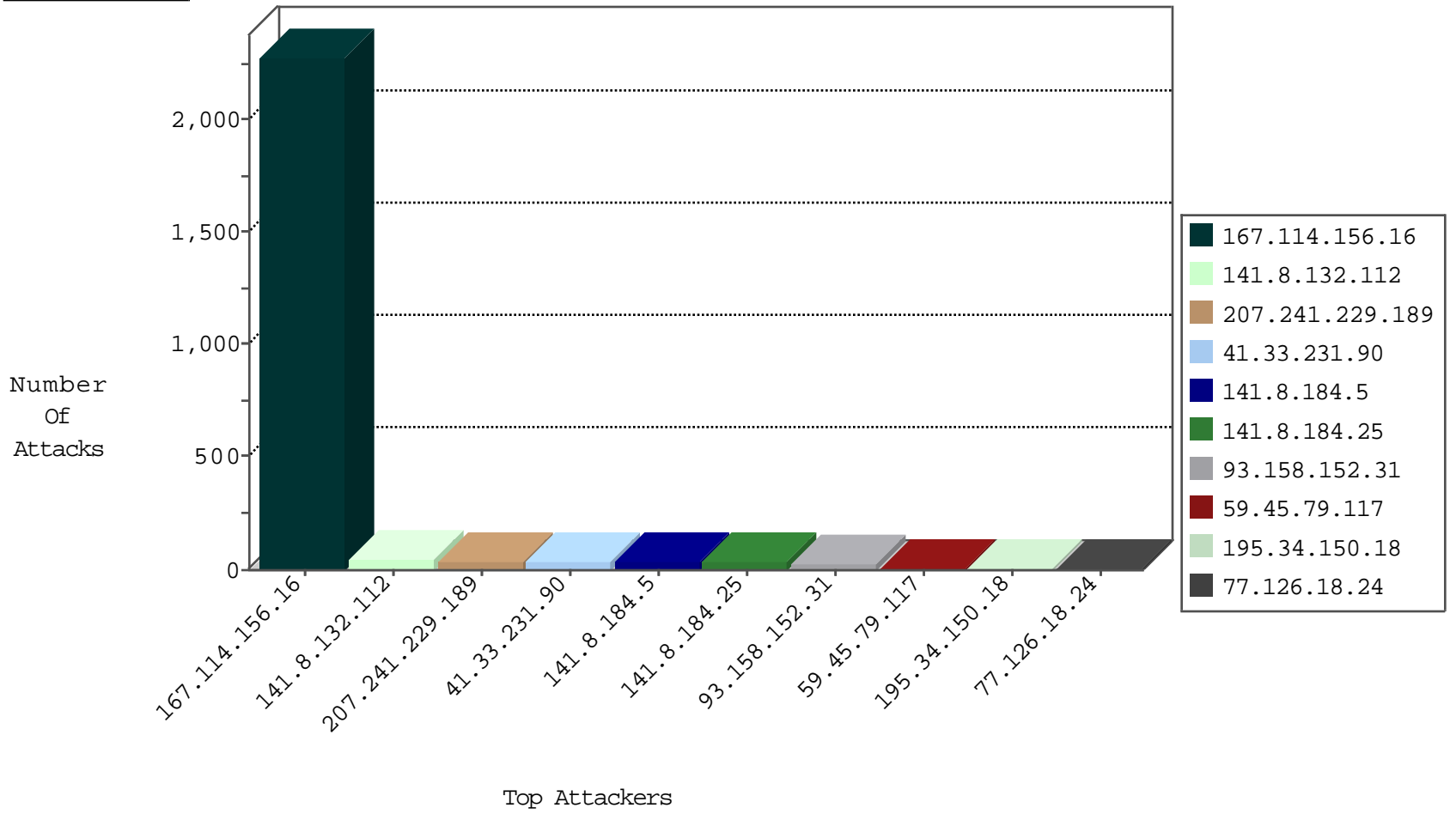
IDF Under Attack Daily Report



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	3131
202.116.234.16	China	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
23.95.54.18	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
23.95.54.18	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.159	China	147.237.77.233	atal.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
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
54.214.251.35	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
218.246.0.97	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
1.54.162.25	147.237.8.14	Vietnam	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
199.191.56.188	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
198.20.69.77	147.237.72.166	United States	aka.idf.il	ET DROP Dshield Block Listed Source	1
108.168.185.133	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.120	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN NMAP -sS window 1024	1
210.146.207.142	147.237.76.34	Japan	yohalan.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.188	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
207.241.229.189	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
141.8.184.5	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
141.8.184.25	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
93.158.152.31	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	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
79.176.72.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
68.180.229.239	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.237.82.50	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.79.10	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
208.115.111.68	United States	147.237.77.74	law.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
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.206	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.108.80.128	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
37.204.149.159	Russian Federation	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.102	United States	147.237.0.33	idf.il	drop		drop	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
81.169.237.146	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
46.19.86.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.20.69.74	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.207	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.6	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.89	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
184.105.139.122	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.108.80.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
108.168.185.133	United States	147.237.76.39	mobile.meitav.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.20	United States	147.237.0.33	idf.il	drop		drop	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.247.203	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.108.80.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
108.168.185.133	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
75.186.33.162	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.115.113.89	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
184.105.247.216	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
84.108.80.128	Israel	147.237.77.233	atal.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
52.90.128.17	United States	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	3
157.55.39.57	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
77.126.18.24	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/xmlrpc.php	Block	1
66.249.78.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/gyus/general.aspx	Block	1
197.32.177.158	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
94.59.62.29	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.79.195	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
157.55.39.131	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/imagevideogallerylobby/	Block	1
77.126.18.24	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
66.249.78.160	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/gyus/general.aspx	None	1
198.20.69.77	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
94.59.62.29	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/homepage/asp	Block	1
54.173.223.170	United States	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.146	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
77.126.18.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/gyus/general.aspx	None	1
203.133.171.99	Korea, Republic of	147.237.76.200	eitan.aka.idf.il	Unknown Parameter l in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	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
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.70	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/links/links.aspx	Block	1
190.252.35.104	Colombia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
77.126.18.24	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.79.119	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-he/dover.aspx	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-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/1133-22461-he/dover.aspx.	Block	1
77.126.18.24	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
66.249.64.186	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
197.32.177.158	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
77.126.18.24	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.79.121	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1