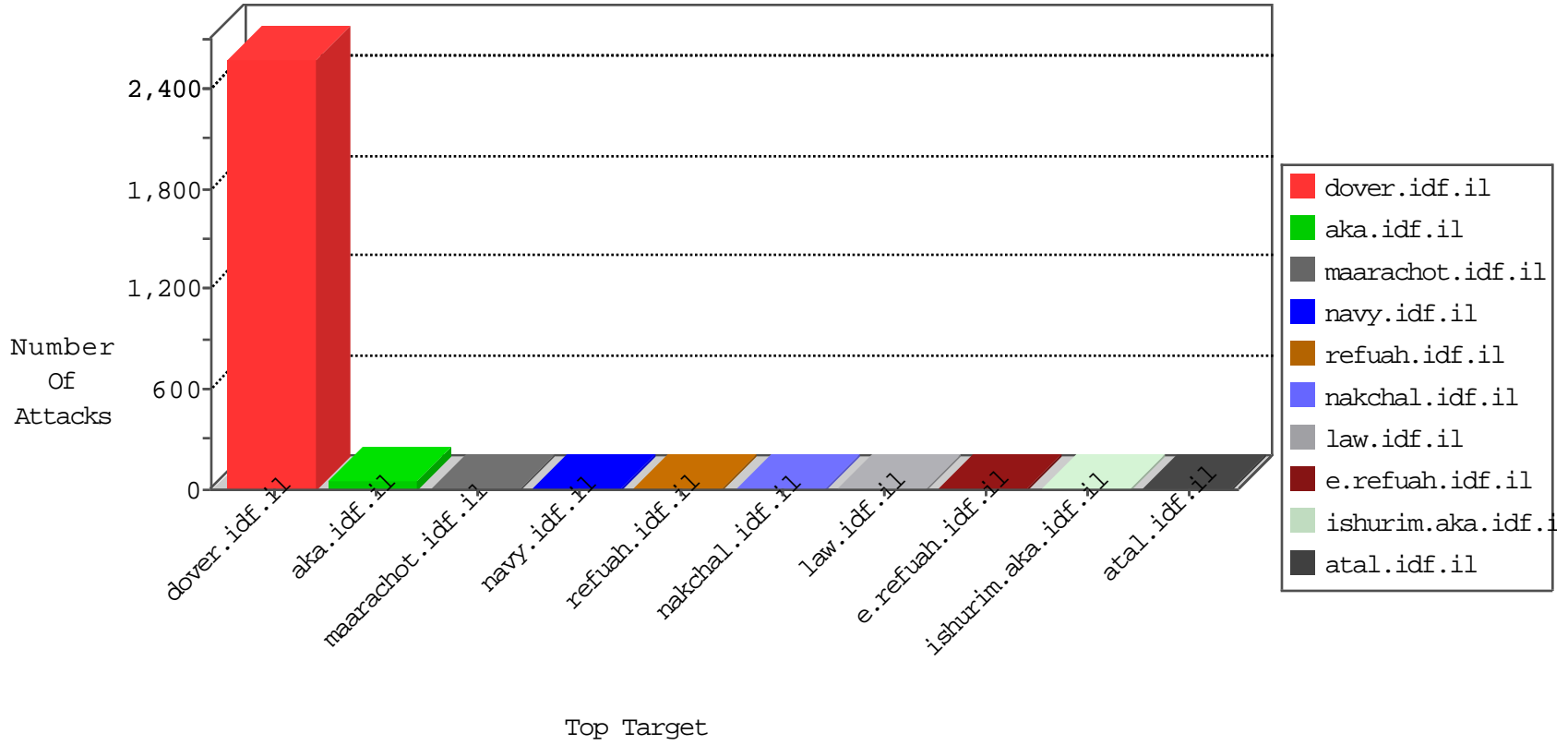


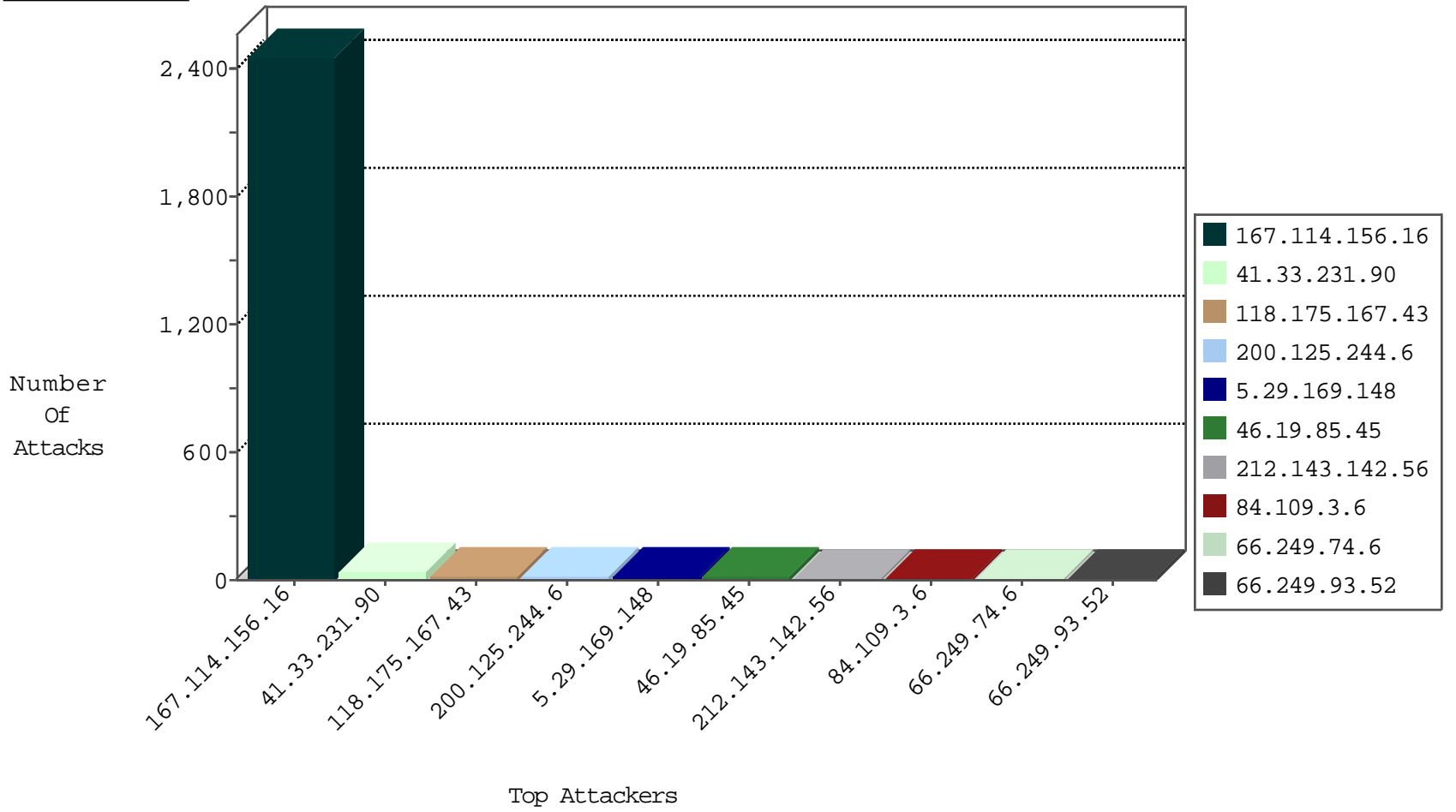
IDF Under Attack Daily Report



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	3419
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	2
159.148.186.181	Latvia	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
71.6.158.166	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
223.73.45.66	China	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
158.69.213.39	United States	147.237.77.176	matpash.idf.il	C1000106: HTTP: majestic bot	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
204.45.15.186	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
121.40.195.144	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.143.102.180	147.237.77.74	Austria	law.idf.il	ET SCAN NMAP -sS window 3072	1
74.203.240.228	147.237.76.148	United States	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
175.143.53.17	147.237.76.44	Malaysia	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
175.143.53.17	147.237.76.44	Malaysia	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
103.251.112.155	147.237.0.15	Hong Kong	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.143.102.180	147.237.77.74	Austria	law.idf.il	ET SCAN NMAP -sS window 1024	1
74.203.240.228	147.237.76.148	United States	ggcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
175.143.53.17	147.237.76.44	Malaysia	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	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
118.175.167.43	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
200.125.244.6	Ecuador	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.74.6	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.52	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
200.125.244.6	Ecuador	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.109.3.6	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.29.169.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.61.123	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.169.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
37.26.148.212	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.20	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
74.82.47.36	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.111	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.99	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.109.73.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
199.127.226.150	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
146.185.239.102	Russian Federation	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.76	United States	147.237.0.33	idf.il	drop		drop	1
74.82.47.36	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.200	United States	147.237.76.147	chimuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.105	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.109.73.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.76	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.208.205.43	United States	147.237.72.156	aman.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
46.19.85.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.203	United States	147.237.8.27	e.nadim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.106	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.148.212	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.75	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.77	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.109.3.6	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.211	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.122	United States	147.237.0.33	idf.il	drop		drop	1
74.82.47.35	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.91	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.98	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.74	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.22.129.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.123	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.75	United States	147.237.0.33	idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.182.144.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 107.178.194.79	Block	2
5.29.169.148	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.29.169.148	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.184.112.74	Block	2
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1396-he/atal.aspx	Block	1
5.29.169.148	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/sip_storage/files/7	Block	1
199.127.226.150	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
74.208.205.43	United States	147.237.72.156	aman.idf.il	E-mail collector robots 14	Block	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1398-he/atal.aspx	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
107.178.194.87	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2400.jpg	Block	1
5.29.169.148	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	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
74.208.205.43	United States	147.237.72.156	aman.idf.il	eMail Hoarding	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20422-he/idfgdover.aspx	Block	1
223.73.45.66	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
141.212.122.97	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /x	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2427.jpg	Block	1
207.46.13.30	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
223.73.45.66	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
178.91.16.171	Kazakstan	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/faq.aspx	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
46.166.139.20	Netherlands	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
207.46.13.150	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/7/	Block	1
66.249.64.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1400-he/atal.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19278-he/kkkkkkk=2aa22d8bkkkkkkk_2aa22d8b	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8910-he/refuah.aspx	Block	1
46.166.139.20	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1