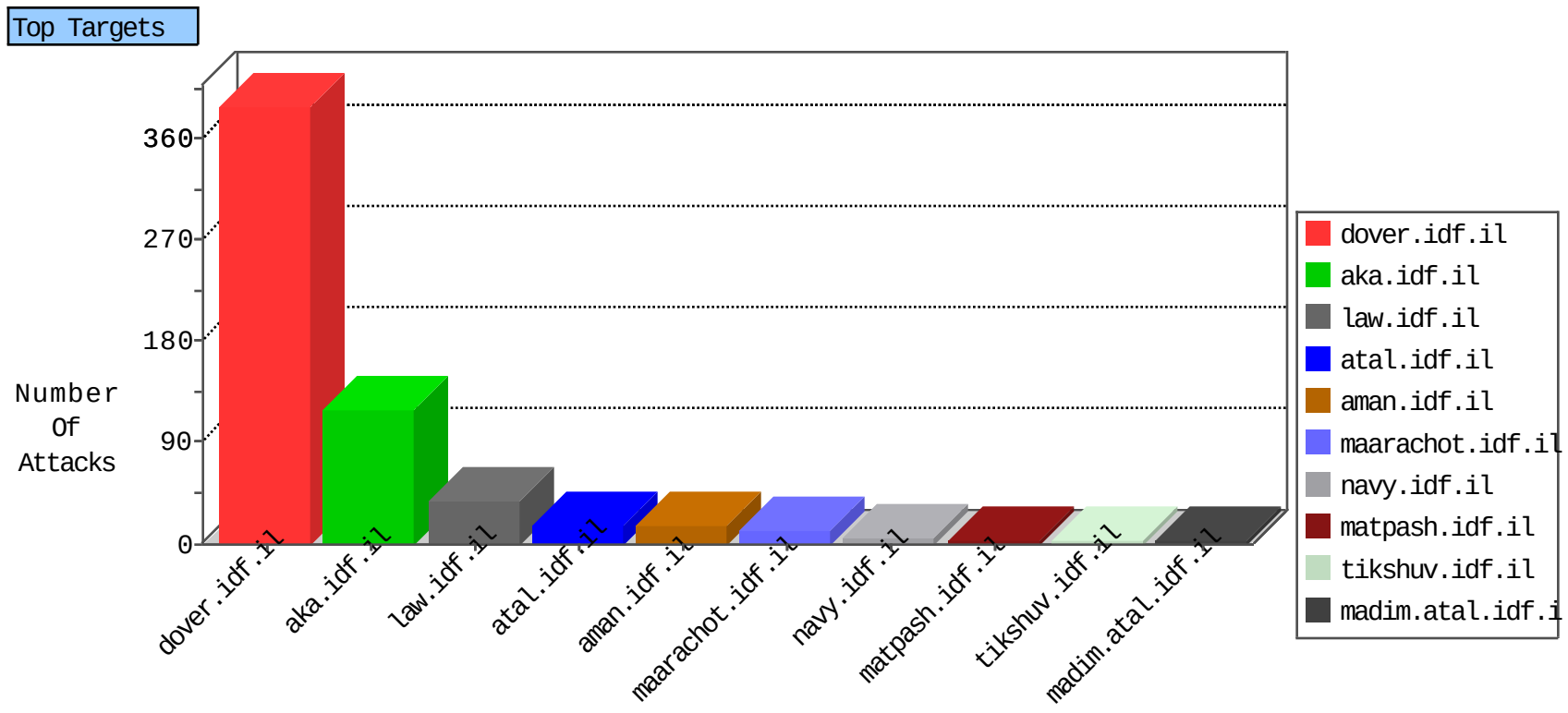
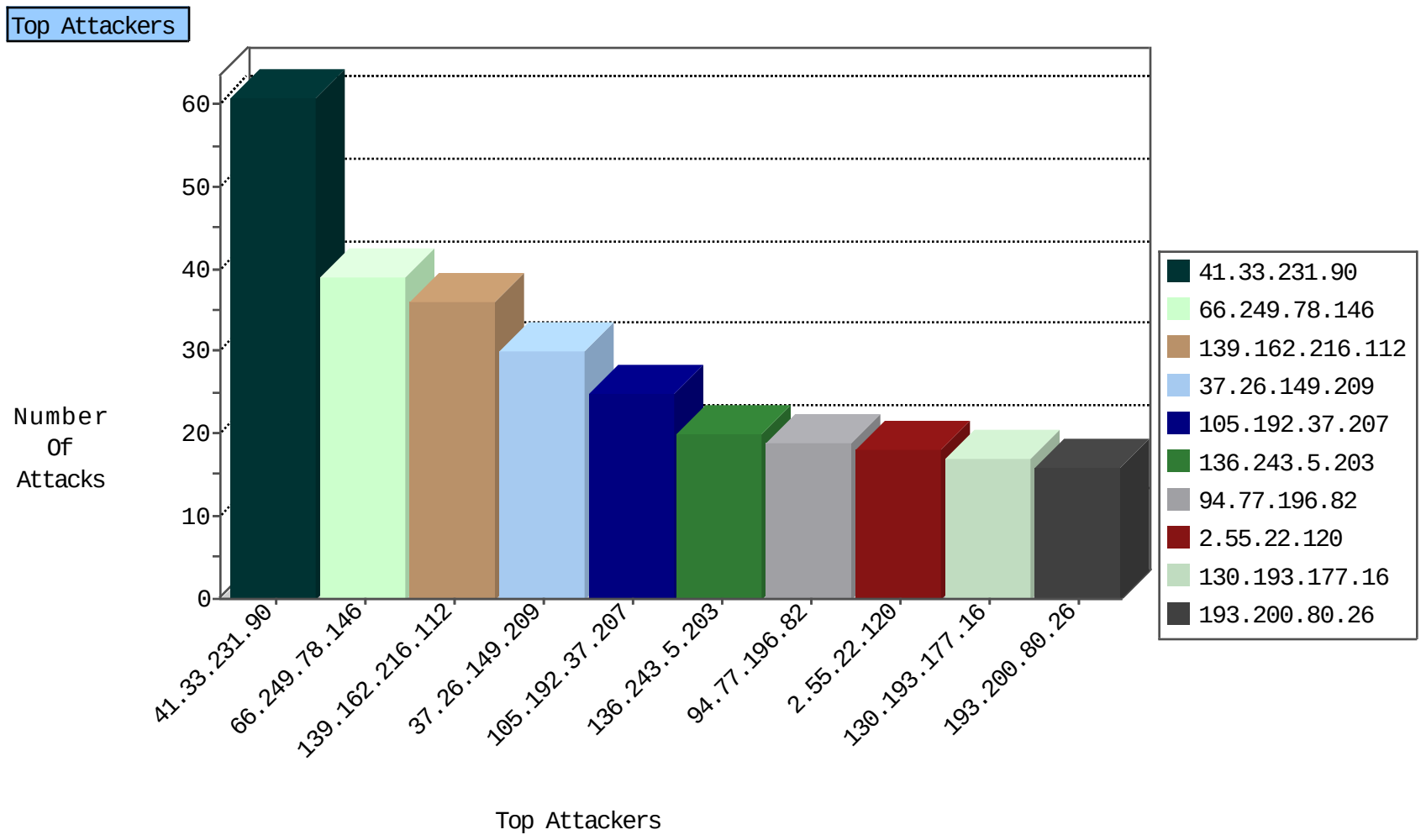
04-22-2016-21:04:07 to 04-22-2016-22:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-22-2016-21:04:07 to 04-22-2016-22:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	131
212.29.192.143	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
2.53.5.27	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
198.20.69.98	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

04-22-2016-21:04:07 to 04-22-2016-22:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.200.80.26	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

04-22-2016-21:04:07 to 04-22-2016-22:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
193.200.80.26	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.246.130.127	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
66.249.64.124	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
183.60.48.25	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
110.143.44.114	147.237.0.200	Australia	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.211.11	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
110.143.44.114	147.237.76.148	Australia	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
104.219.238.10	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.76	147.237.76.196	Turkey	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1

04-22-2016-21:04:07 to 04-22-2016-22:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
139.162.216.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
105.192.37.207	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	21
136.243.5.203	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
130.193.177.16	Iraq	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
157.55.39.230	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
198.58.102.155	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
68.180.231.43	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
109.253.147.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
159.53.174.142	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
208.115.113.89	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
37.26.149.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
207.46.13.14	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
37.26.149.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
45.35.64.142	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
37.26.149.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
157.55.39.91	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
37.26.149.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.149.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
208.115.111.73	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
72.9.148.10	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	4
79.177.204.196	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
52.21.170.167	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
83.244.51.203	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
149.88.204.32	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
66.87.133.3	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
79.181.155.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.224.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.22.120	Israel	147.237.77.216	dover.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
2.53.13.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.55.22.120	Israel	147.237.77.216	dover.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
66.102.6.147	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3
109.253.134.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.22.120	Israel	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	alert	3
2.55.22.120	Israel	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.253.139.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.22.120	Israel	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.54	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
66.249.93.249	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.214	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3

04-22-2016-21:04:07 to 04-22-2016-22:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.29.192.143	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.29.192.143	Block	2
89.238.188.119	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.238.188.119	Block	2
2.53.20.228	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
207.46.13.116	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
109.254.29.48	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
68.180.230.218	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
46.19.86.248	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
203.127.96.213	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
107.150.32.61	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.yun.ph/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
12.199.98.28	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 12.199.98.28	Block	1
130.185.155.10	Sweden	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
74.91.18.44	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
203.127.96.215	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
107.150.32.62	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
66.249.78.140	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/enlarge.asp	Block	1
17.142.149.167	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
212.29.192.143	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/general/mobile	Block	1
130.185.155.10	Sweden	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
74.91.20.198	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
66.249.64.203	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
203.127.96.249	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.65.26.243	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-he/cogat.aspx	Block	1
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/coordinationgaza/news_gaza/pages/tidroohitonaeim.aspx	Block	1
40.77.167.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
220.255.148.142	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.212.122.161	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.75.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
207.46.13.14	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.254.29.48	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
46.19.85.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.88.204.32	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
89.238.188.119	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
66.249.78.13	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1

04-22-2016-21:04:07 to 04-22-2016-22:04:07