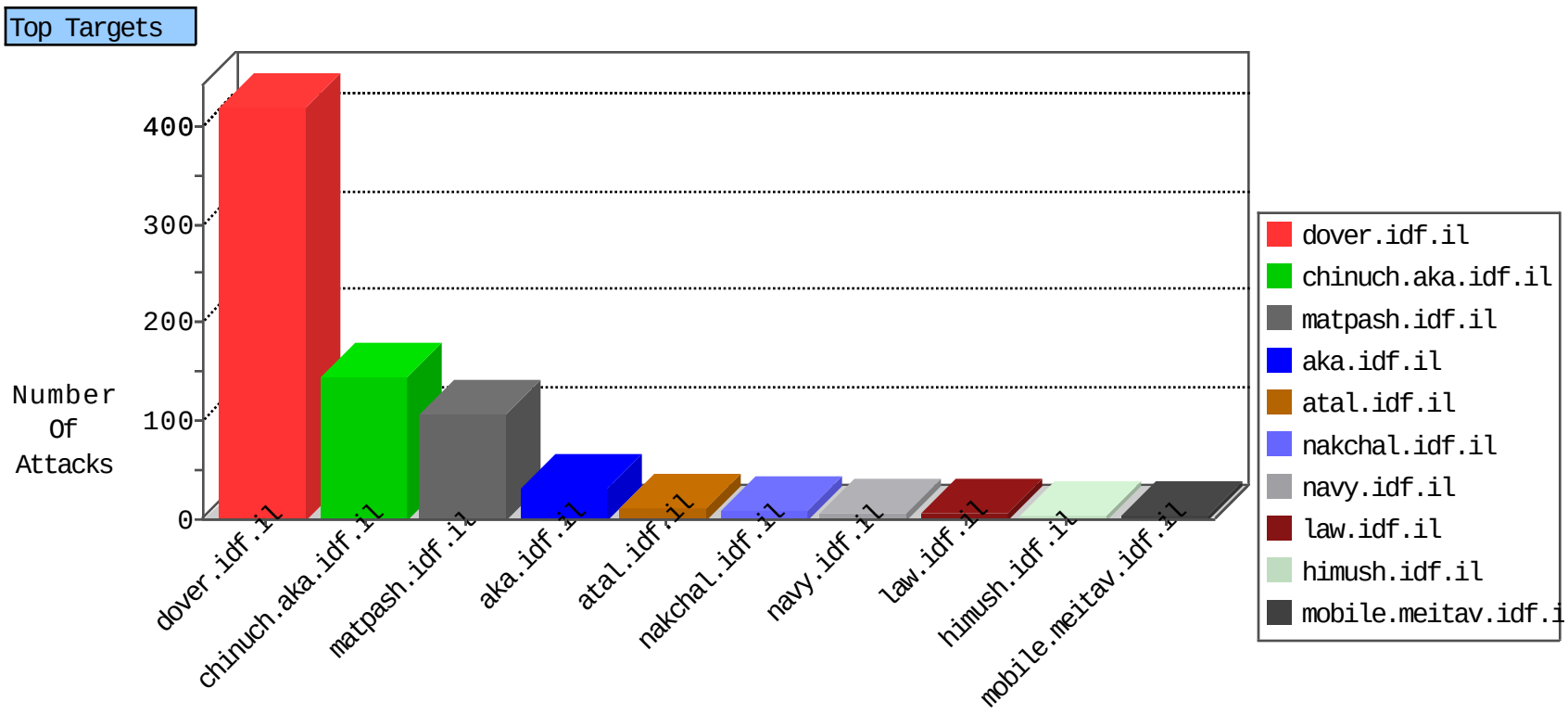
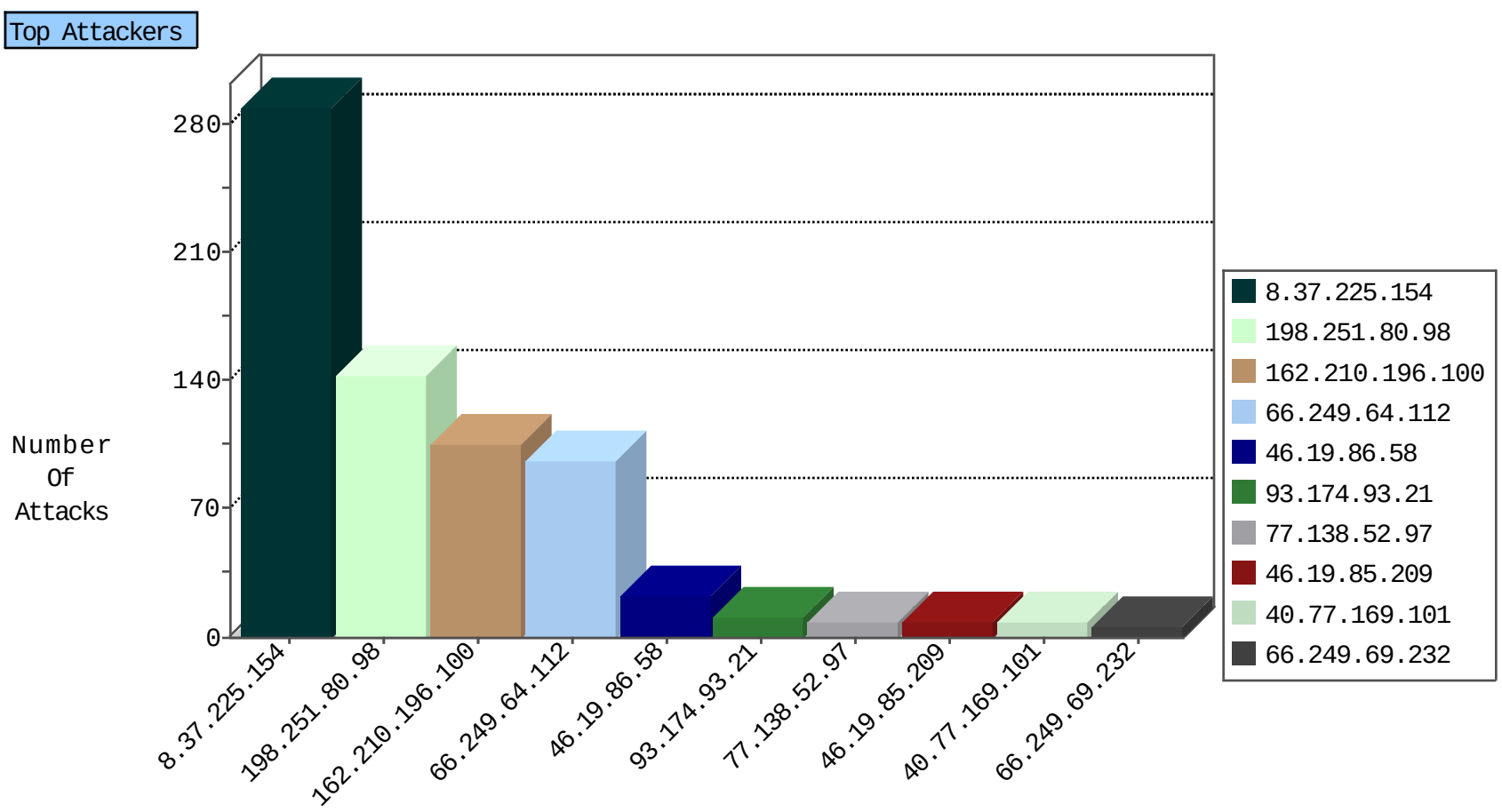
09-24-2016-06:04:07 to 09-24-2016-07:04:07

IDF Under Attack Daily Report



Top Target



Top Attackers

09-24-2016-06:04:07 to 09-24-2016-07:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
40.77.169.101	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
68.180.231.57	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
66.249.69.232	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
45.35.64.142	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
8.37.225.154	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
63.141.242.198	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
63.141.242.196	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
173.208.197.205	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
63.141.231.214	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
204.12.220.82	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
69.30.226.219	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
204.12.220.85	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
69.30.227.219	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
63.141.242.196	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
198.204.224.234	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
45.63.53.164	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
208.110.84.69	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
69.30.227.222	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
63.141.242.198	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
198.204.224.236	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
69.30.193.250	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1

09-24-2016-06:04:07 to 09-24-2016-07:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	65
162.210.196.100	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	24
162.210.196.100	United States	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	8
162.210.196.100	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	6
162.210.196.100	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-24-2016-06:04:07 to 09-24-2016-07:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.112	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	96
27.72.57.38	147.237.77.216	Vietnam	dover.idf.il	Xenu Link Sleuth User Agent	2
180.213.5.205	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
60.179.175.22	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
179.43.141.221	147.237.72.217	Switzerland	e.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.21	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
93.174.93.21	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
93.174.93.21	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
93.174.93.21	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
93.174.93.21	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
188.204.118.102	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
93.174.93.21	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
185.153.198.10	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
180.93.246.2	147.237.0.16	Vietnam	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
139.162.187.89	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.21	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
93.174.93.21	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
93.174.93.21	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
93.174.93.21	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
93.174.93.21	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
185.153.198.10	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	147.237.77.170	Turkey	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1

09-24-2016-06:04:07 to 09-24-2016-07:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.154	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	237
8.37.225.154	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	49
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	36
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	34
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
46.19.86.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.58	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.58	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.209	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
177.23.177.146	Brazil	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	3
46.19.85.209	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.94.60.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.69.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
84.94.60.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
97.33.67.228	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.209	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
187.61.109.18	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
184.105.247.247	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
218.22.211.69	China	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
198.199.89.155	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
45.35.64.142	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.139.110	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.250	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
139.162.37.147	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
66.249.69.232	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.85.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.119	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.232.110.28	United Kingdom	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
199.30.17.49	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.32.179.74	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.32	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.222	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
128.232.110.28	United Kingdom	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	1
78.40.225.156	Turkey	147.237.72.156	aman.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
212.143.142.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
40.77.169.101	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.139.110	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
125.77.28.26	China	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.38	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.247	United States	147.237.0.33	idf.il	drop		drop	1

09-24-2016-06:04:07 to 09-24-2016-07:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	3
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	2
78.40.225.156	Turkey	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/8/70768.jpg	Block	1
207.46.13.143	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
213.151.35.213	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/kamlar/klali/default.asp	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2690.jpg	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/piwik.php	Block	1
66.249.64.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	1
157.55.39.255	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1

09-24-2016-06:04:07 to 09-24-2016-07:04:07