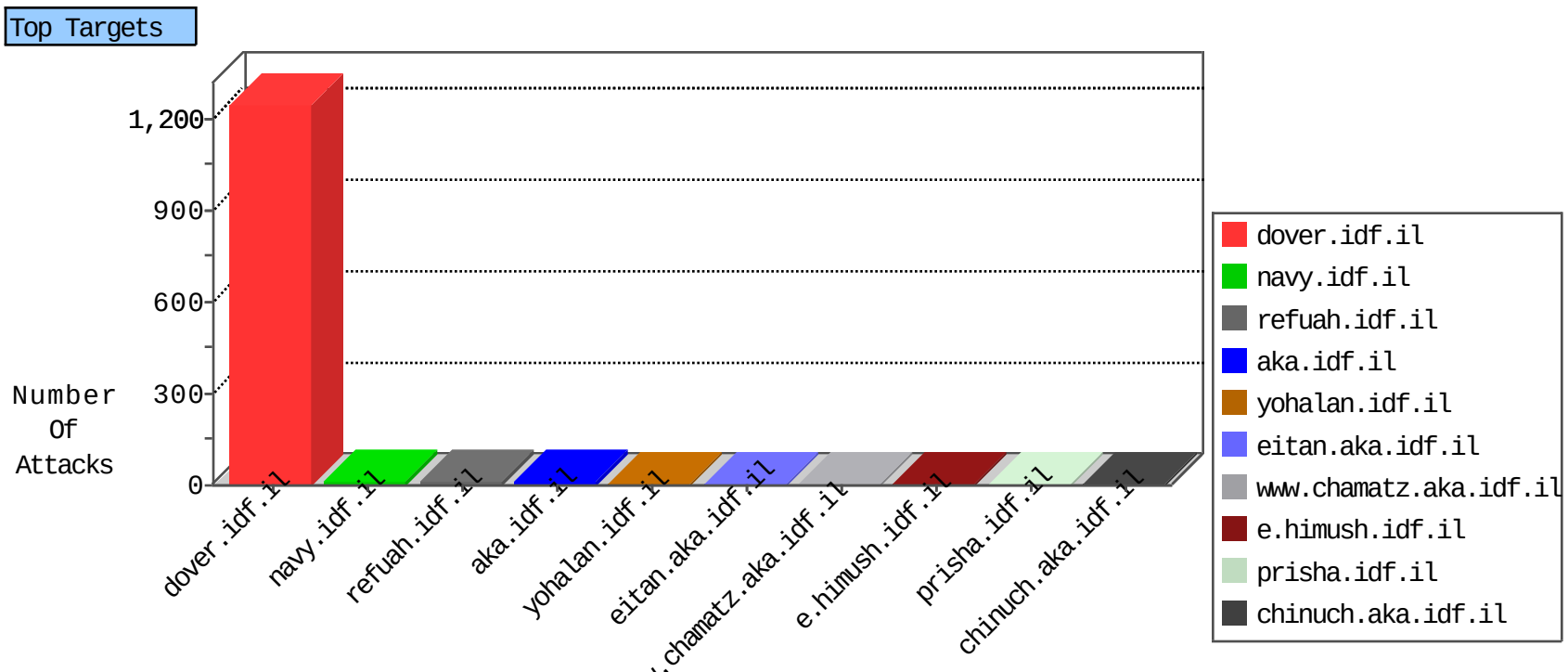
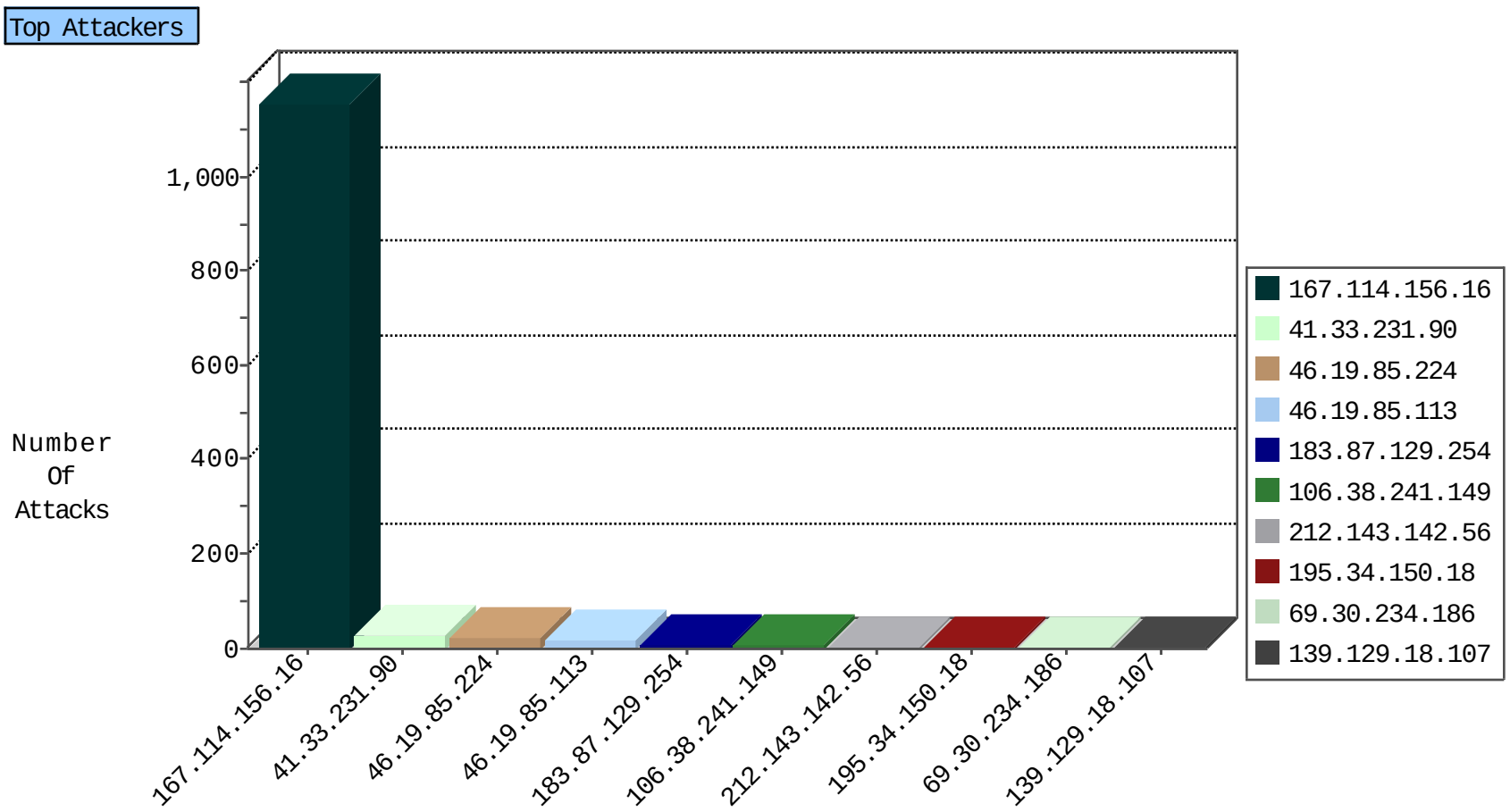
04-15-2016-05:04:02 to 04-15-2016-06:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-15-2016-05:04:02 to 04-15-2016-06:04:02

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	Block_Ip_Web_In	drop	1154
184.105.139.76	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.2	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.84	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.2	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.112	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
82.221.105.6	Iceland	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

04-15-2016-05:04:02 to 04-15-2016-06:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	6
69.30.213.82	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.234.186	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.234.186	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
40.77.167.4	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-15-2016-05:04:02 to 04-15-2016-06:04:02

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
87.229.116.42	147.237.77.226	Hungary	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
40.114.42.13	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
23.96.109.87	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
218.200.188.213	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.221	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
198.71.54.46	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	1
113.196.182.86	147.237.76.147	Taiwan	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
97.74.4.26	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
23.96.109.87	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
218.200.188.213	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
23.96.109.87	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
199.101.186.221	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
199.101.186.221	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -f -sS	1
198.71.54.46	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
165.138.213.4	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
113.196.182.86	147.237.76.147	Taiwan	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1

04-15-2016-05:04:02 to 04-15-2016-06:04:02

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	30
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.224	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.224	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.113	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
183.87.129.254	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
139.129.18.107	China	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
46.19.85.113	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
183.87.129.254	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
208.115.113.88	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
151.80.31.172	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
183.87.129.254	India	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
74.82.47.23	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.100	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.250	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.130	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
84.108.70.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.86	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.187.114.171	France	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.88	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.24	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.112	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
104.238.169.116	United Kingdom	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.51	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.92	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
183.87.129.254	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.91	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.55	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
172.58.217.244	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.51	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.98	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.92	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.56	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.76	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
50.153.156.226	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.100	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.248	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.129	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
79.181.214.165	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.78	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
14.175.223.165	Vietnam	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
183.87.129.254	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.87	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

04-15-2016-05:04:02 to 04-15-2016-06:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.46.13.140	United States	147.237.77.216	dover.idf.i	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.i	Unauthorized URL Access to 147.237.77.216/1133-20222-he/dover.aspx	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.i	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.i	Unauthorized URL Access to 147.237.77.216/1133-20313-he/dover.aspx	Block	1
204.79.180.16	United States	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp	Block	1
204.79.180.161	United States	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
204.79.180.234	United States	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/haredim/general.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1

04-15-2016-05:04:02 to 04-15-2016-06:04:02