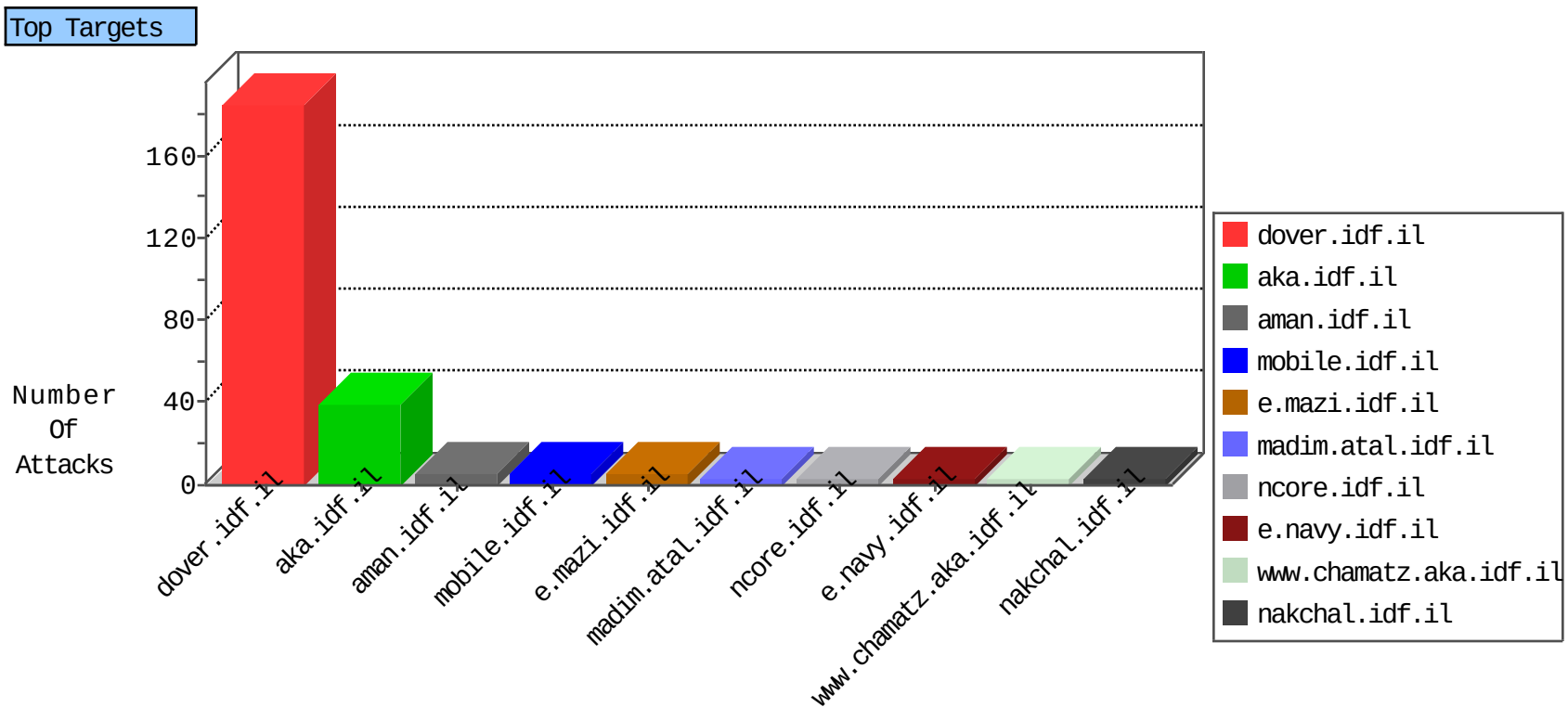
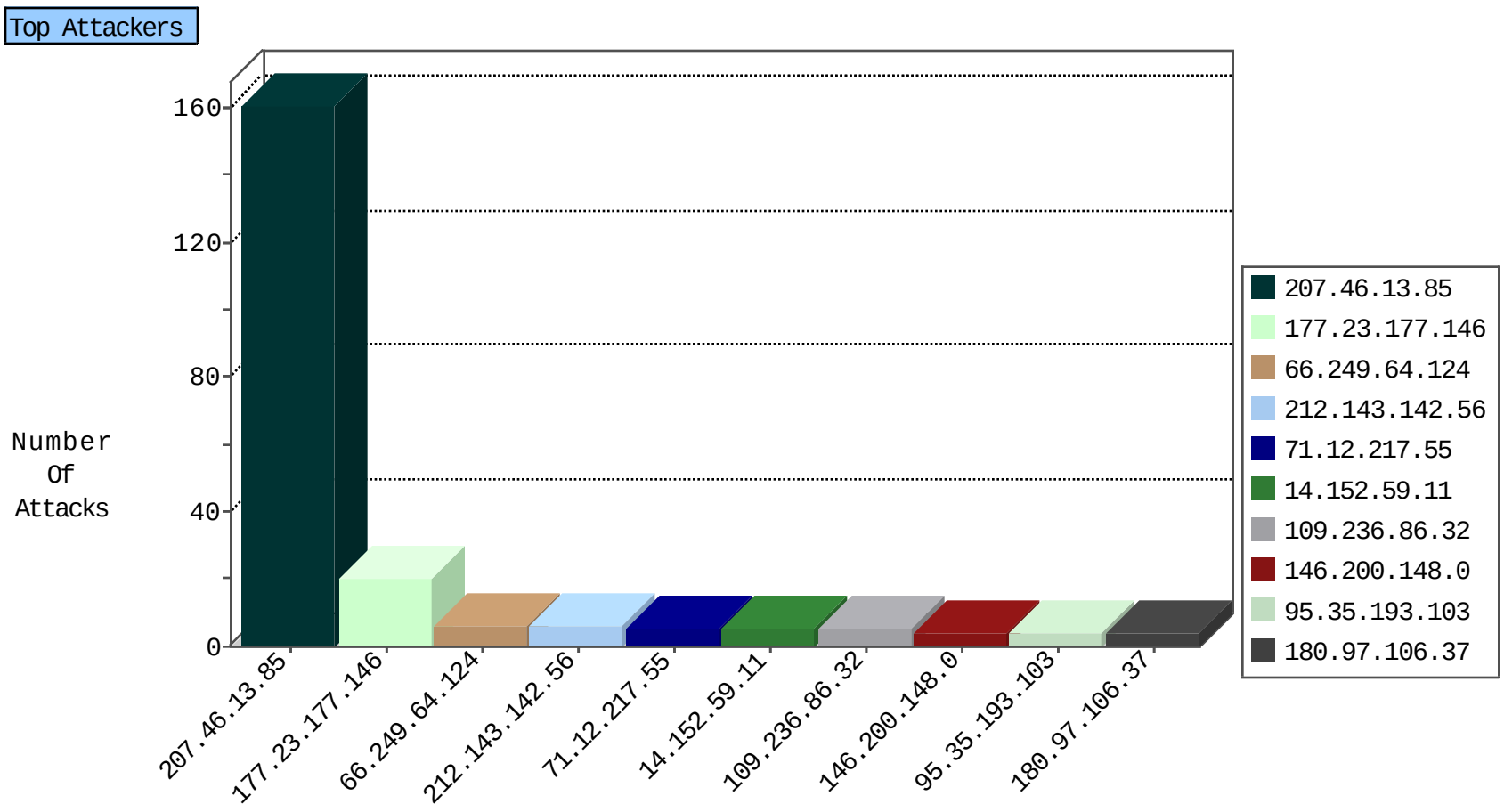
10-05-2016-04:04:07 to 10-05-2016-05:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-05-2016-04:04:07 to 10-05-2016-05:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.65.154	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
78.129.171.175	United Kingdom	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
121.12.170.153	China	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
78.129.171.175	United Kingdom	147.237.76.201	e.atal.idf.il	Black List	drop	1
95.67.136.219	Russian Federation	147.237.76.177	ncore.idf.il	ID-OpenSSL-Heartbeat-ex1	dest-reset	1

10-05-2016-04:04:07 to 10-05-2016-05:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
163.172.32.175	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	1

10-05-2016-04:04:07 to 10-05-2016-05:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
146.200.148.0	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
45.76.2.156	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
206.116.149.159	147.237.72.167	Canada	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
45.76.2.156	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
14.152.59.11	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.236.86.32	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.236.86.32	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
52.57.110.155	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
52.57.110.155	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
46.249.82.10	147.237.77.205	Bulgaria	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
45.76.2.156	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
14.152.59.11	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
117.168.110.253	147.237.72.217	China	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.236.86.32	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.236.86.32	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
106.75.9.82	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
52.57.110.155	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
46.249.82.10	147.237.77.205	Bulgaria	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
209.126.230.71	147.237.76.177	United States	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-05-2016-04:04:07 to 10-05-2016-05:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
207.46.13.85	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	160
177.23.177.146	Brazil	147.237.72.166	aka.idf.il	Header Rejection	header rejection pattern found in request	monitor	18
66.249.64.124	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
71.12.217.55	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
113.175.215.201	Vietnam	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.11.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.240.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.67.69.166	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
95.35.193.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
217.132.37.229	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
208.54.36.230	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
95.35.193.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
45.56.74.212	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
180.97.106.37	China	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.246.121	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
14.152.59.11	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.226.113.7	Germany	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.139.116	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
23.239.31.132	United States	147.237.77.227	e.hamaz.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
139.162.160.132	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.74	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
45.56.74.212	United States	147.237.77.121	e.navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
180.97.106.161	China	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
14.152.59.11	China	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.86	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
137.226.113.7	Germany	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
198.58.110.199	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
23.239.31.132	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
180.97.106.37	China	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.160.132	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
104.237.146.151	United States	147.237.76.199	e.nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.85.187	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
180.97.106.161	China	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
14.152.59.11	China	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.87	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
45.33.124.223	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
180.97.106.37	China	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.102.195.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
139.162.168.200	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.85.187	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.162	China	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
23.92.20.154	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.87	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
73.153.73.3	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
45.33.124.223	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
180.97.106.37	China	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
139.162.168.200	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

10-05-2016-04:04:07 to 10-05-2016-05:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.229.178	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/chamatz	Block	1
66.249.64.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8688-he/refuah.aspx	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1401-he/atal.aspx	Block	1
66.249.79.38	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/born2.htm	Block	1
66.249.76.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/7/שקופית6	Block	1

10-05-2016-04:04:07 to 10-05-2016-05:04:07