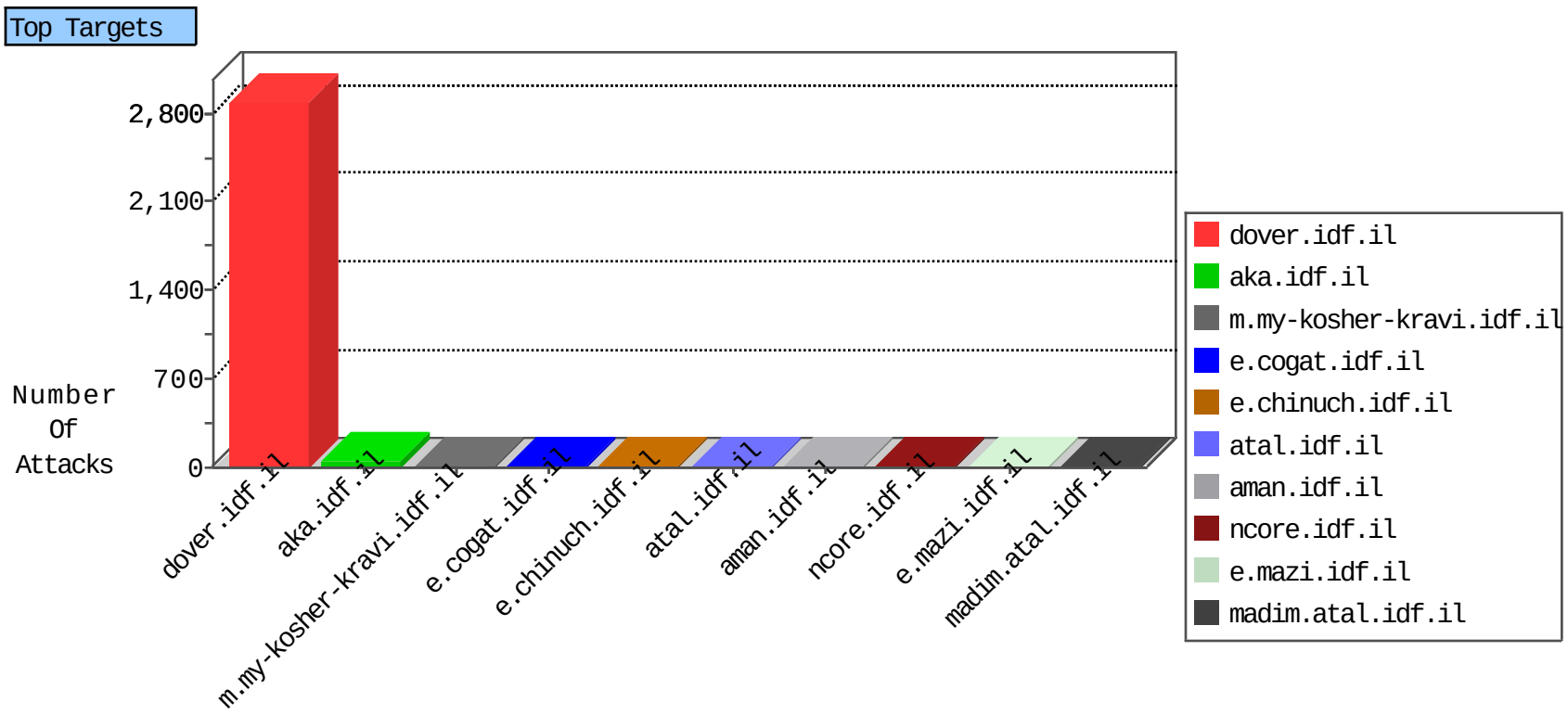
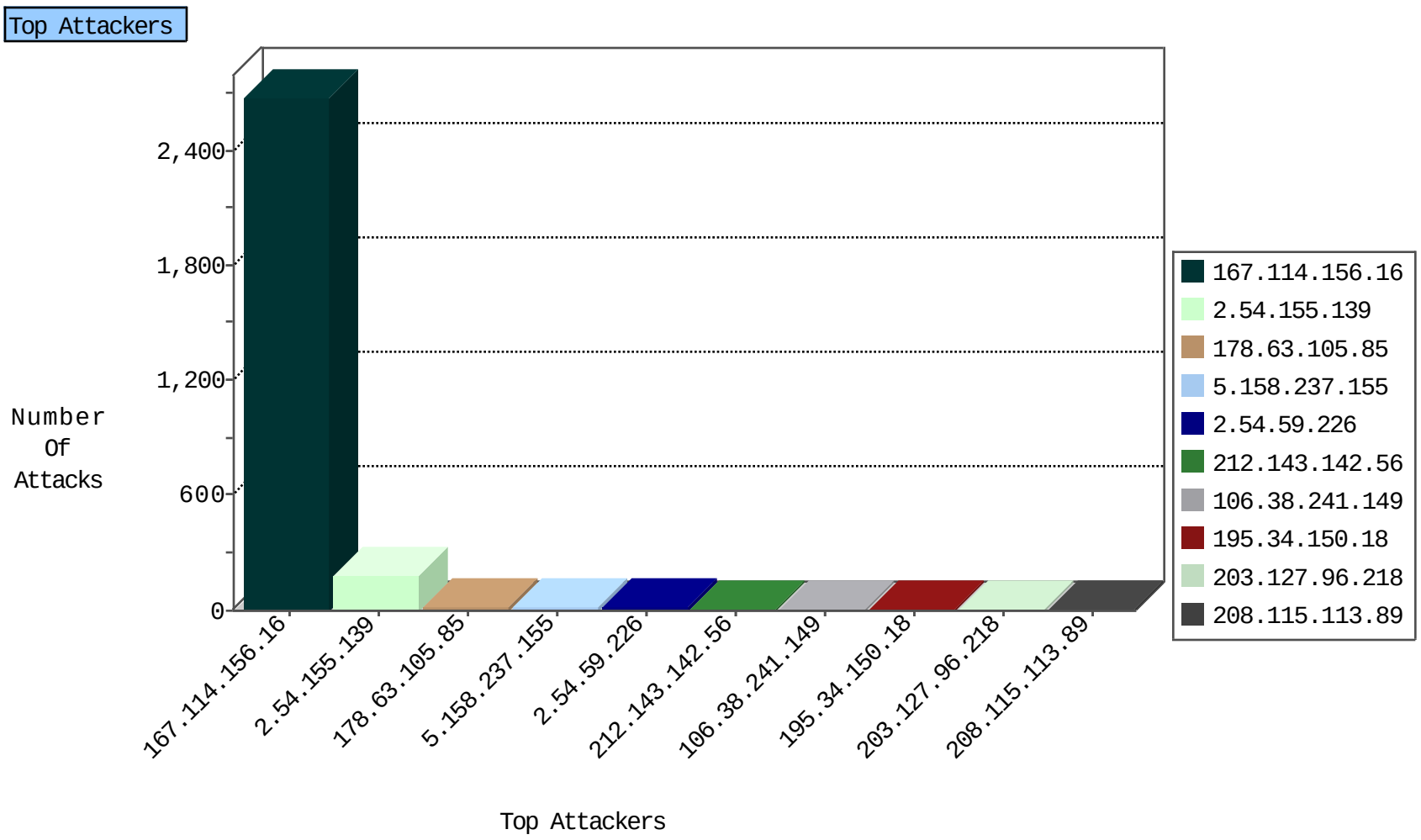
03-16-2016-02:04:01 to 03-16-2016-03:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-16-2016-02:04:01 to 03-16-2016-03:04:01

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	3495
115.28.27.173	China	147.237.76.44	e.refuah.idf.il	Invalid TCP Flags	drop	1
104.239.173.81		147.237.8.45	e.eitan.idf.il	L4 Source or Dest Port Zero	drop	1
110.76.40.33	China	147.237.8.28	e.mobile-ks.idf.il	Invalid TCP Flags	drop	1
180.97.31.70	China	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid L4 Header Length	drop	1
114.215.193.117	China	147.237.0.17	m.my-kosher-kravi.idf.il	L4 Source or Dest Port Zero	drop	1

03-16-2016-02:04:01 to 03-16-2016-03:04:01

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	4
212.83.177.193	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
46.165.197.142	Germany	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
188.165.15.23	France	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-16-2016-02:04:01 to 03-16-2016-03:04:01

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
218.246.0.97	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.221	147.237.72.14		dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
74.208.238.221	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
187.189.118.25	147.237.77.233	Mexico	atal.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.76.198	Turkey	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
13.71.146.233	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1

03-16-2016-02:04:01 to 03-16-2016-03:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	32
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
2.54.59.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	4
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	4
2.54.7.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	3
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	2
5.102.242.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	2
132.64.142.38	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.46.41.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
192.118.60.69	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.88.89.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.177.43.209	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.4.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.99	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.63.105.85	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
141.212.122.149	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
38.229.1.15	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
197.38.175.202	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
159.226.95.66	China	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.149	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
188.34.204.45	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
178.63.105.85	Germany	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
141.212.122.150	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.160	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.218	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
119.29.153.110	China	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
188.34.204.45	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.169	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.11	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.218	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
120.132.67.209	China	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.118.60.69	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.170	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.11	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
203.127.96.218	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
178.63.105.85	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1

03-16-2016-02:04:01 to 03-16-2016-03:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.155.139	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 2.54.155.139	Block	169
2.54.155.139	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.54.155.139	Block	8
5.158.237.155	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
5.158.237.155	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.158.237.155	Block	5
207.46.13.105	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
185.32.179.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.65	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/894-he/אגף הטכנולוגיה והלוגיסטיקה.aspx	Block	1
66.249.78.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
208.115.113.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/hebrew/asp/default.asp	Block	1
119.73.253.4	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.158.237.155	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
2.54.155.139	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/71659.not	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
183.12.97.154	China	147.237.77.216	dover.idf.il	Illegal URL Path Encoding www.idf.il/english%	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
91.143.197.224	Italy	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sviva	Block	1
66.249.78.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main/faq.asp	Block	1
207.46.13.160	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
91.143.197.224	Italy	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
220.255.146.231	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
203.127.58.235	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-9301-he/dover.aspx	Block	1
207.46.13.192	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
95.86.74.64	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/1151-he/chinuch.aspx&sa=u&ved=0ahukewi785cx9splahvldjokhw8bcrgqfggmmai&sig2=aeedif2zbuqrndzpkulbja&usg=afqjcney99eefhkfwifkkrltvuw9op3qya	Block	1

03-16-2016-02:04:01 to 03-16-2016-03:04:01