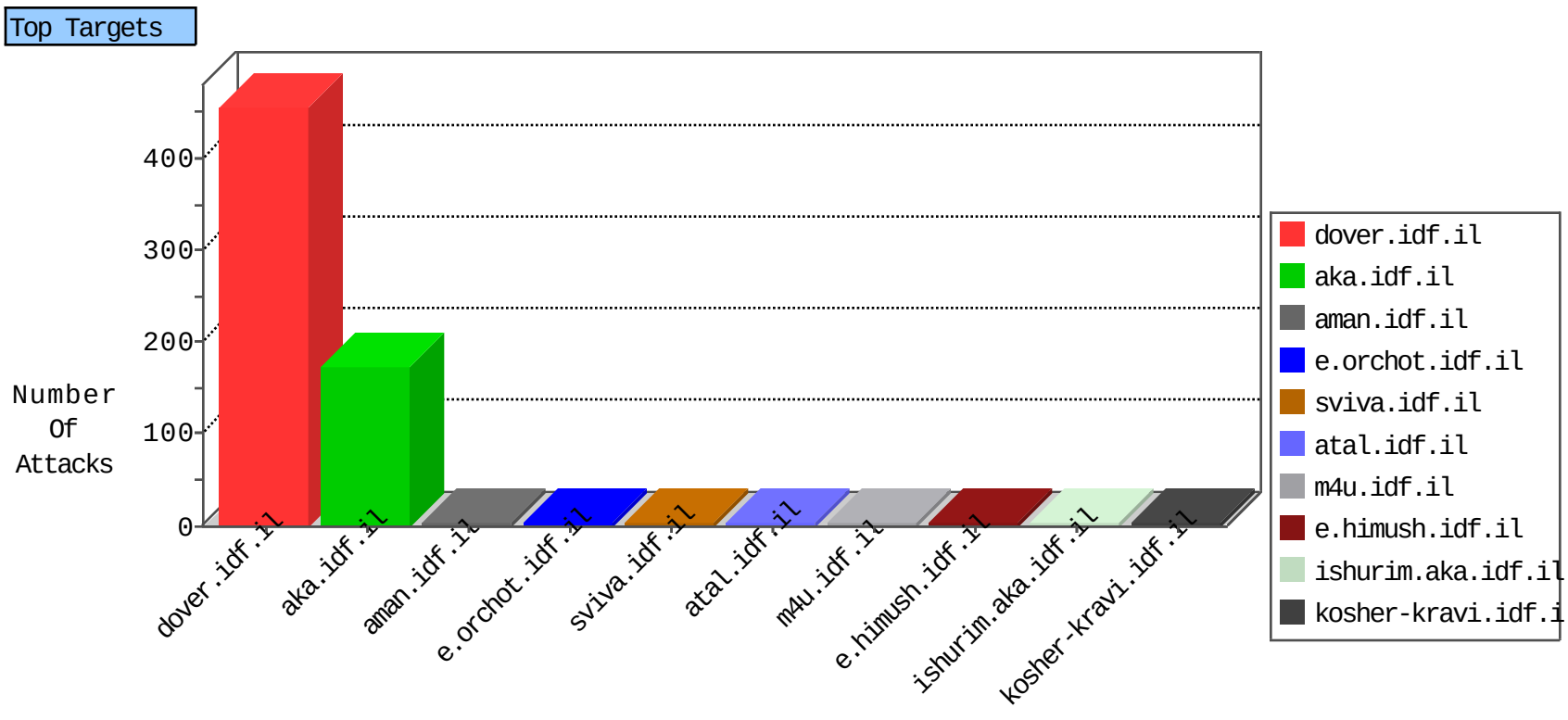
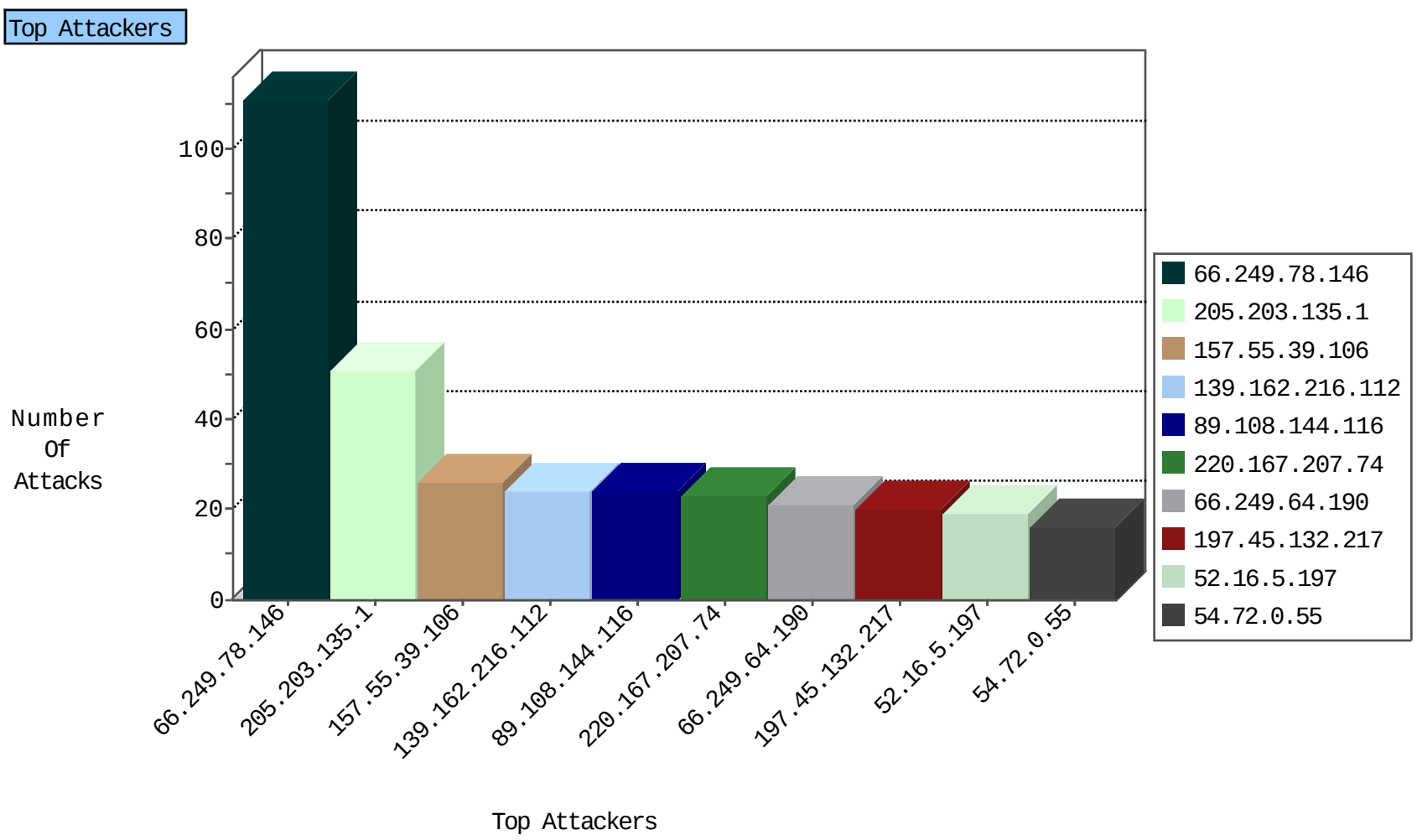
04-29-2016-04:04:09 to 04-29-2016-05:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-29-2016-04:04:09 to 04-29-2016-05:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.146	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
23.239.65.178	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

04-29-2016-04:04:09 to 04-29-2016-05:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.169.156.247	United States	147.237.77.216	dover.idf.i	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	1
52.169.156.247	United States	147.237.77.216	dover.idf.i	19863: HTTP: WordPress Revslider/Showbiz PHP File Upload	Block	1

04-29-2016-04:04:09 to 04-29-2016-05:04:09

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
220.167.207.74	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	2
220.167.207.74	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
220.167.207.74	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
52.169.156.247	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2
220.167.207.74	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
220.167.207.74	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
220.167.207.74	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
220.167.207.74	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
76.181.249.213	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
220.167.207.74	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
220.167.207.74	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
220.167.207.74	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
220.167.207.74	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
179.43.144.43	147.237.72.167	Switzerland	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
220.167.207.74	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
220.167.207.74	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential SSH Scan	1
220.167.207.74	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1
220.167.207.74	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
220.167.207.74	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
220.167.207.74	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
220.167.207.74	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
220.167.207.74	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	1
220.167.207.74	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	1

04-29-2016-04:04:09 to 04-29-2016-05:04:09

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	108
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
89.108.144.116	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.99.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.116.30.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
217.23.14.168	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.203.135.93	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
70.50.134.139	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
128.242.249.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
87.69.255.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
71.94.241.223	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
71.161.84.174	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
108.84.131.20	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
204.237.2.151	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
172.56.7.193	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.91.40.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
70.27.216.9	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.206	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
99.31.227.98	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
173.252.115.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.29.66.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.125.142.136	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
157.55.12.69	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
199.30.16.161	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
193.33.226.10	Russian Federation	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
52.169.156.247	United States	147.237.77.216	dover.idf.il	Application Servers Protection Violation	PhpMyAdmin SERVER Superglobal Remote Variable Manipulation - Detect over uploaded data	monitor	2

04-29-2016-04:04:09 to 04-29-2016-05:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.169.156.247	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
52.169.156.247	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 52.169.156.247	Block	2
2.53.150.53	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
54.188.186.80	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1379-he/dover.aspx parameter PageNum	Block	1
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/home/default.aspx	None	1
52.169.156.247	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
144.76.64.79	Germany	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
54.203.135.93	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1379-he/dover.aspx parameter PageNum	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
157.55.39.134	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
54.212.79.196	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1927-en/cogat.aspx gaza semanales	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
163.172.129.70	United Kingdom	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
54.244.162.211	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1379-he/dover.aspx parameter PageNum	Block	1
79.183.119.213	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
52.169.156.247	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-admin/admin-post.php	Block	1
207.46.13.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/asp/iturimpages.asp	Block	1
52.12.14.230	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1379-he/dover.aspx parameter PageNum	Block	1

04-29-2016-04:04:09 to 04-29-2016-05:04:09