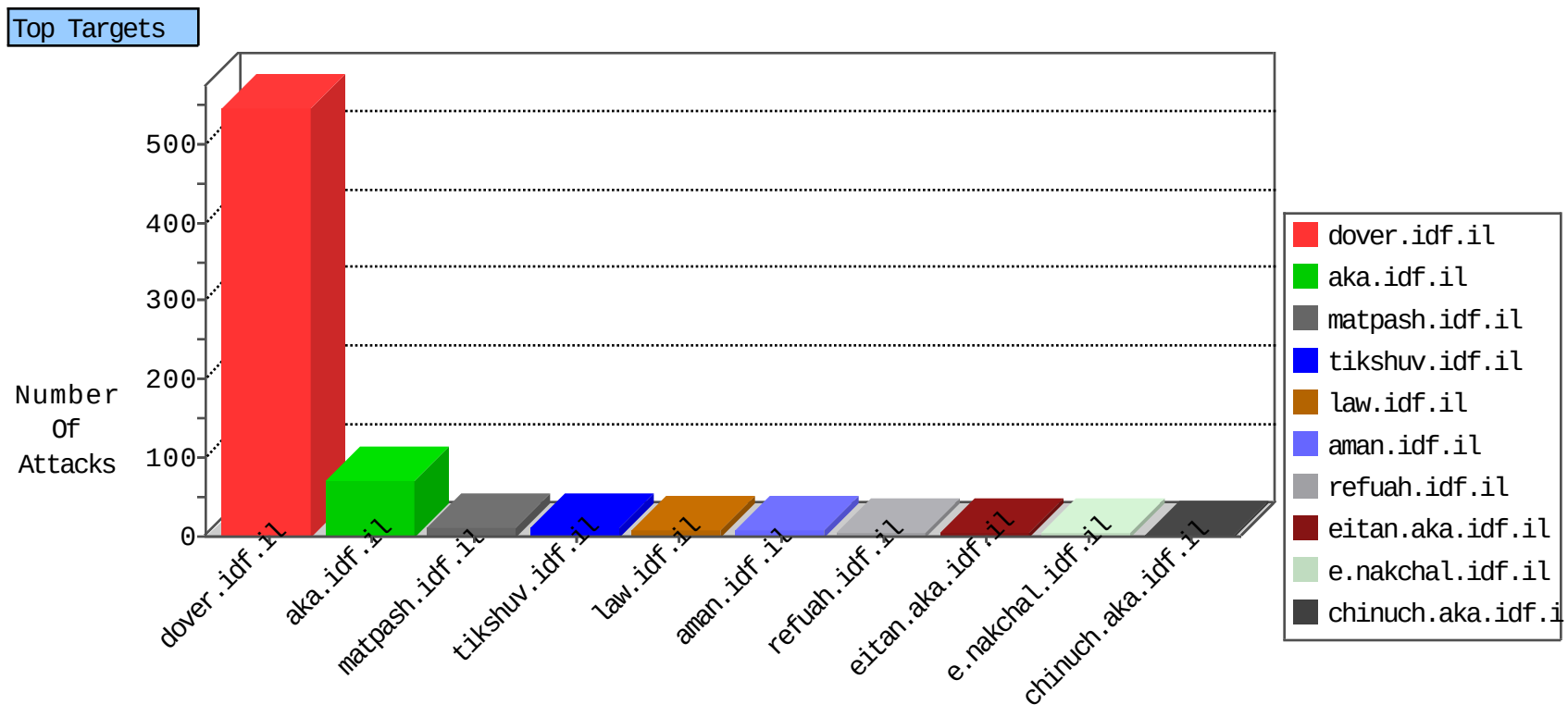
05-01-2016-05:04:05 to 05-01-2016-06:04:05

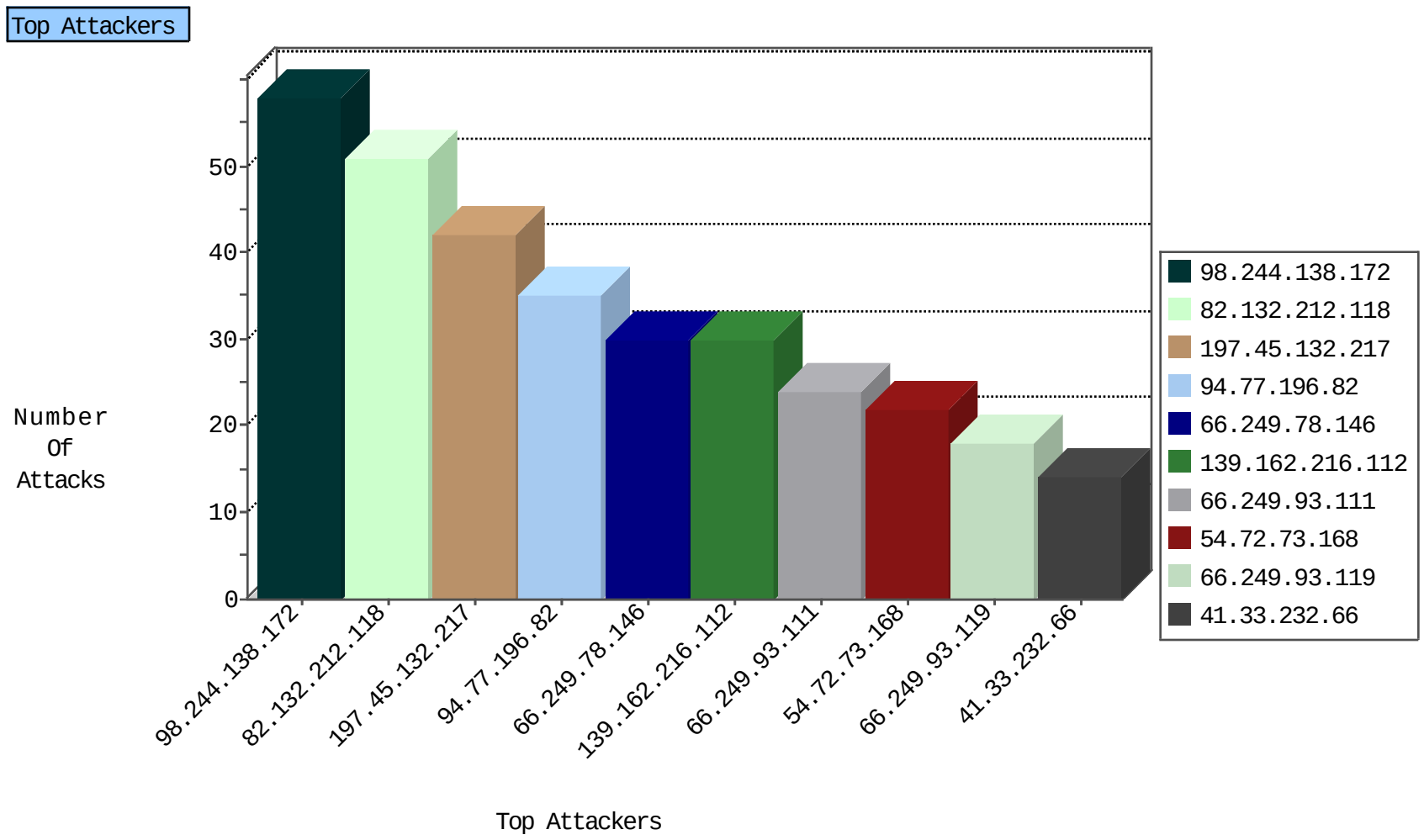
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

05-01-2016-05:04:05 to 05-01-2016-06:04:05

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	7
185.94.111.1	Russian Federation	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

05-01-2016-05:04:05 to 05-01-2016-06:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-01-2016-05:04:05 to 05-01-2016-06:04:05

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
89.248.167.131	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
130.211.77.81	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.155	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.155	147.237.76.199	Ukraine	e.nakchal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
89.248.167.131	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.72.156		aman.idf.il	ET SCAN NMAP -sS window 1024	1
130.211.77.81	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.155	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
89.248.167.131	147.237.77.235	Netherlands	sviva.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
89.248.167.131	147.237.76.177	Netherlands	ncore.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

05-01-2016-05:04:05 to 05-01-2016-06:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
98.244.138.172	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
82.132.212.118	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
162.243.99.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.212.105.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.12.102.90	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
82.132.212.118	United Kingdom	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
68.180.231.43	United States	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	8
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
130.203.136.75	United States	147.237.77.74	law.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	8
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.5.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
172.56.13.160	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.64.177	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.252.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.199	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.152.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.50	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
177.207.4.157	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.64.176	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.225.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.54.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

05-01-2016-05:04:05 to 05-01-2016-06:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.223.122	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	2
198.58.103.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
74.82.47.4	United States	147.237.0.19	madim.atal.idf.i	Distributed Unauthorized URL Access on 147.237.0.19/	Block	1
207.46.13.145	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/faq/	Block	1
173.153.21.177	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/894-he/eitan.aspx	None	1
66.249.66.84	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
201.202.125.150	Costa Rica	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
173.153.21.177	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/mobile	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/71582.pdf	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
94.159.165.33	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
184.105.247.195	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
68.180.229.226	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/7/1437.pdf/	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jump_2_eng_300900.stm)	Block	1
156.170.173.22	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.154.152.197	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 185.3.144.33	Block	1
68.180.230.108	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
207.46.13.55	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in aka.idf.il/main/giyus/	None	1
160.176.135.239	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.64.80	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/מאיר שחaspx.מו	Block	1

05-01-2016-05:04:05 to 05-01-2016-06:04:05