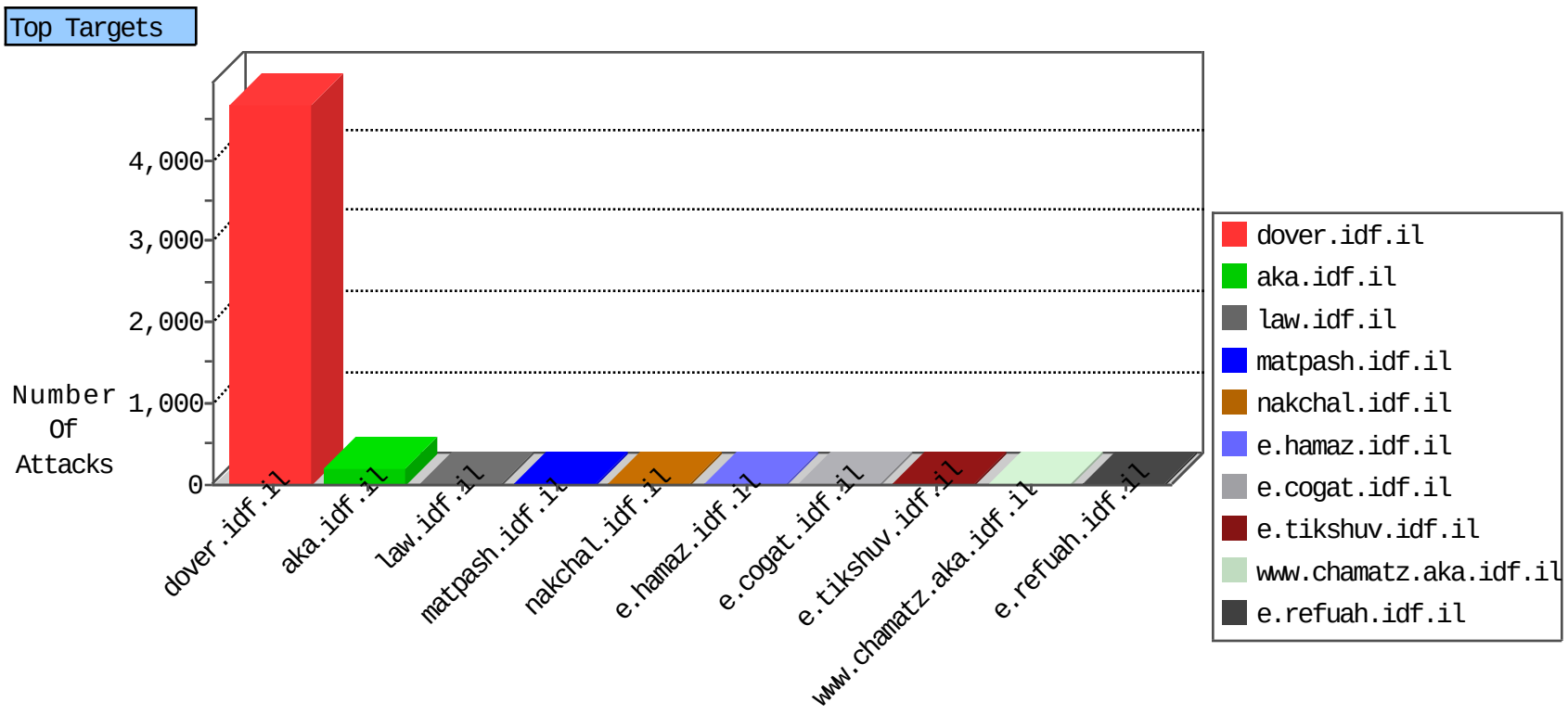
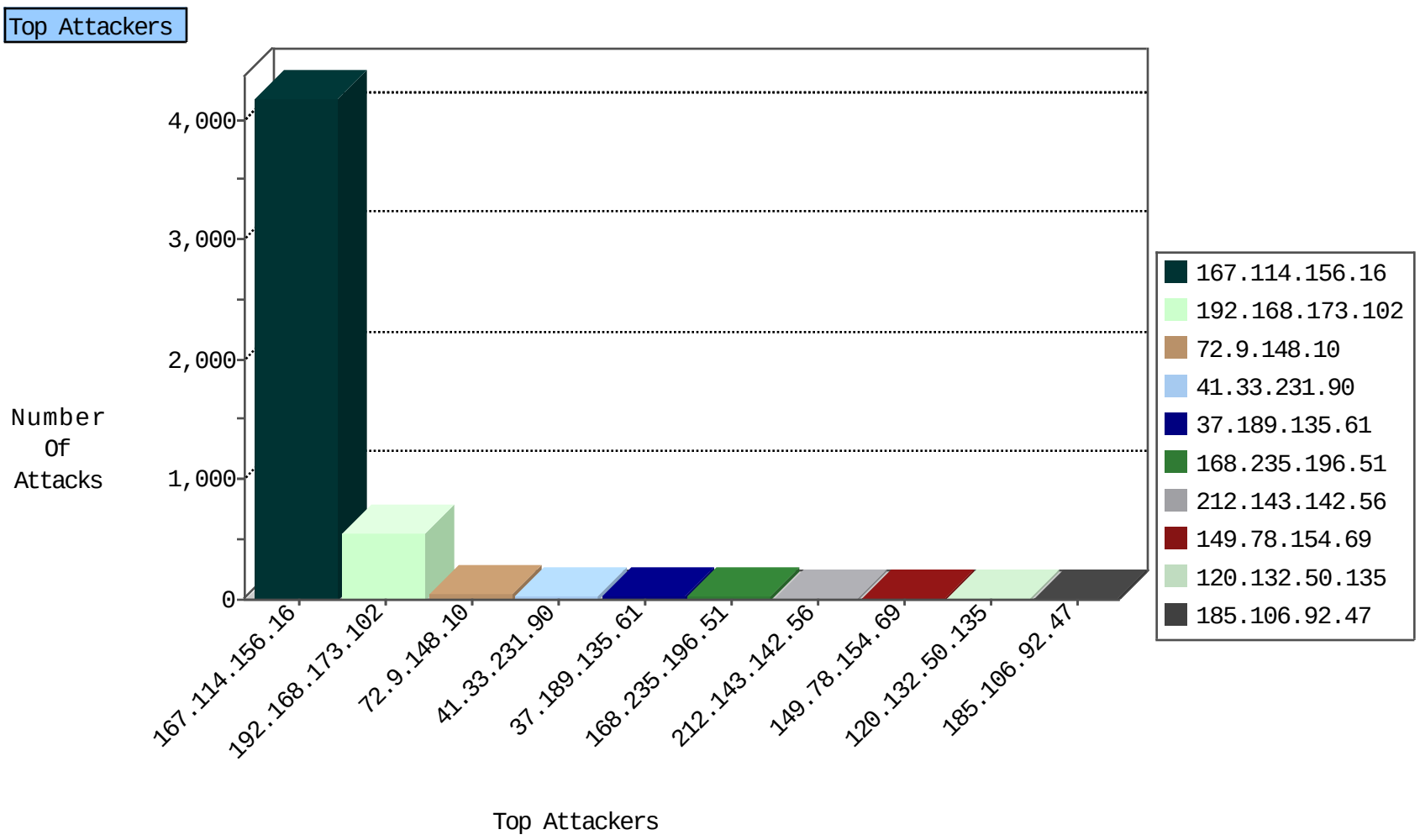
04-08-2016-06:04:07 to 04-08-2016-07:04:07

IDF Under Attack Daily Report





04-08-2016-06:04:07 to 04-08-2016-07:04:07

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	4171
120.132.50.135	China	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	4
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	2
184.105.139.80	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1

04-08-2016-06:04:07 to 04-08-2016-07:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.198.143.123	Ukraine	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	4
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-08-2016-06:04:07 to 04-08-2016-07:04:07

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
80.82.78.38	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.139.45	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
218.108.132.58	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
203.197.205.118	147.237.8.50	India	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
185.103.252.87	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
114.143.103.124	147.237.76.30	India	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.92.139.45	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.139.45	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.77.233	Latvia	atal.idf.il	ET SCAN NMAP -sS window 1024	1
191.14.211.135	147.237.0.33	Brazil	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
179.43.144.37	147.237.76.199	Switzerland	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1

04-08-2016-06:04:07 to 04-08-2016-07:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	356
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	190
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.189.135.61	Portugal	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
168.235.196.51	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	17
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
188.161.55.149	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
147.27.70.36	Greece	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.140.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.80	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.109	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
195.88.209.6	Russian Federation	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
60.242.185.29	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.137.59.78	Morocco	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
176.13.1.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.170	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.107.110.228	Greece	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.106.92.47	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.102.195.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.244	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.170	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.82.78.38	Netherlands	147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1
216.218.206.79	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.106.92.47	Russian Federation	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
157.55.39.205	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.168	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.117.247.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
141.212.122.171	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.82.78.38	Netherlands	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
216.218.206.83	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.169	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.119.112.23	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
185.106.92.47	Russian Federation	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
80.82.78.38	Netherlands	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.100	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.169	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.23	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

04-08-2016-06:04:07 to 04-08-2016-07:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.75.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.169	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1132-8613-he/navy.aspx.aspx	Block	1
80.230.224.17	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.181	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
80.230.224.153	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
120.132.50.135	China	147.237.76.31	nakchal.idf.i	Unauthorized URL Access to www.ctrip.com/894-he/nakhal.aspx	Block	1
40.77.167.25	United States	147.237.76.31	nakchal.idf.i	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
183.198.2.169	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13854-en/dover.	Block	1
54.75.228.43	Ireland	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1

04-08-2016-06:04:07 to 04-08-2016-07:04:07