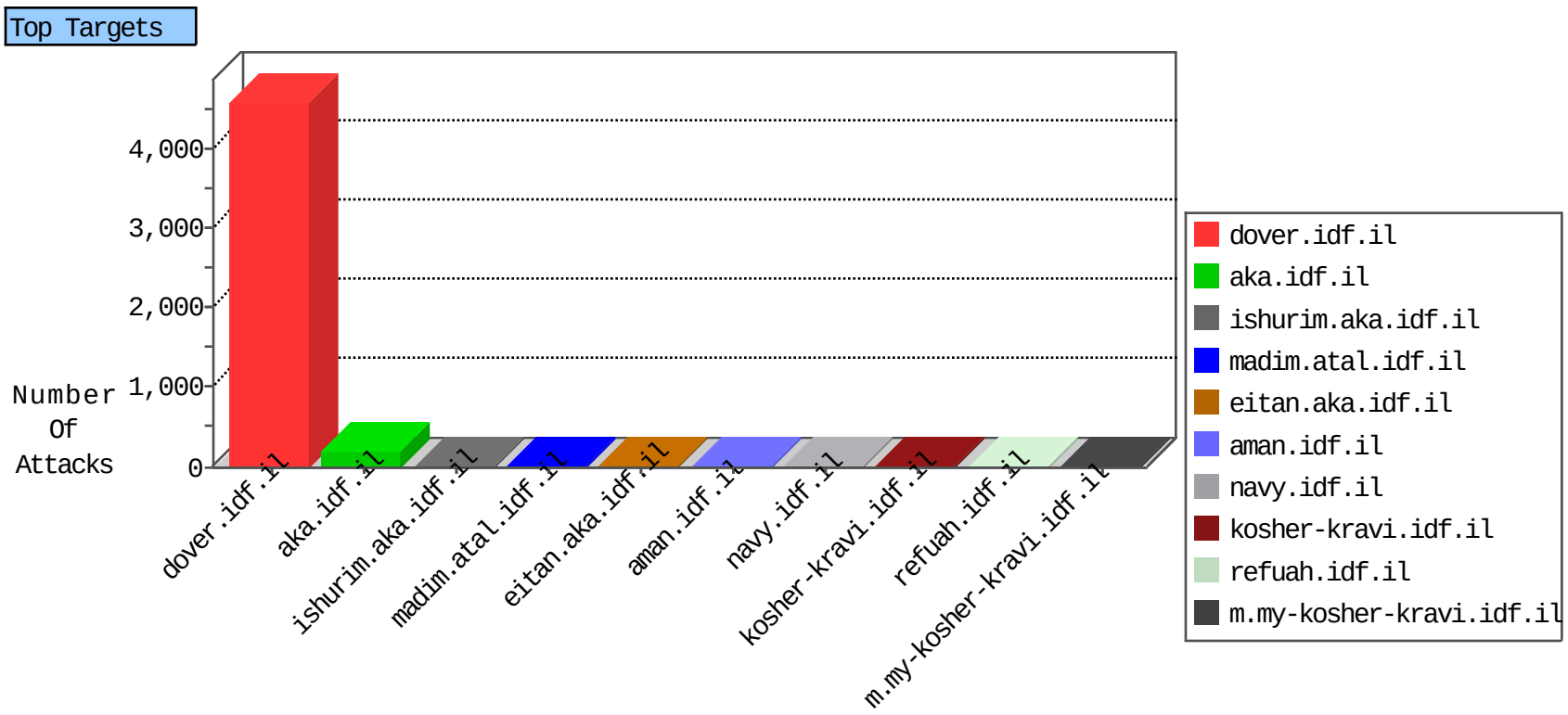
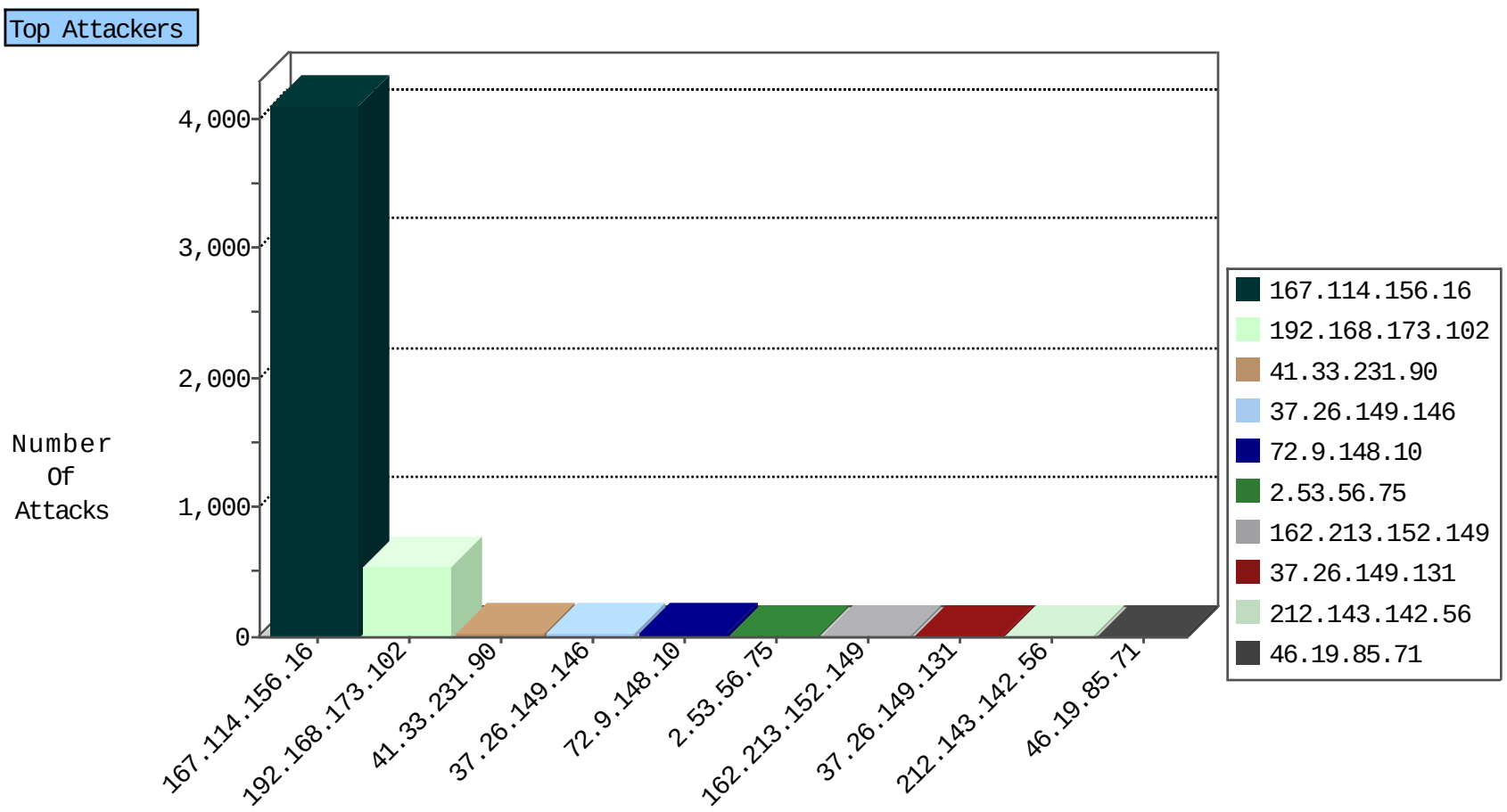
04-08-2016-07:04:08 to 04-08-2016-08:04:08

IDF Under Attack Daily Report





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

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	4099
123.59.59.52	China	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
82.145.218.209	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	2
183.60.48.25	China	147.237.0.200	m4u.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
184.105.139.72	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
185.70.184.164	Netherlands	147.237.77.19	law-forum.idf.il	L4 Source or Dest Port Zero	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
192.3.220.210	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.210.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
178.137.86.10	Ukraine	147.237.72.166	aka.idf.il	C1000016: HTTP: administrator in URI	Block	1
66.249.78.127	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

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

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
213.151.60.89	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
31.210.188.20	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
31.210.188.20	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
104.232.98.3	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
14.115.182.63	147.237.76.202	China	e.halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.92.246.145	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
195.216.176.244	147.237.8.46	Latvia	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
122.49.2.46	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.246.145	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 4096	1

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

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	370
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	180
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.26.149.146	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
37.26.149.131	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.71	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	9
37.26.149.146	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
162.213.152.149	United States	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.3.147.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
162.213.152.149	United States	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	4
199.30.25.68	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
104.172.207.143	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.64.84.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.255	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.171.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	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
162.213.152.149	United States	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	3
104.172.207.143	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.64.172	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.22.129.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
112.95.249.13	China	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	2
31.148.219.11	Netherlands	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
89.139.80.107	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
162.210.196.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
66.249.64.169	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.55.48.200	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
162.213.152.149	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.170	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.106.92.47	Russian Federation	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.106	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.76.216.52	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
162.213.152.149	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
119.9.49.11	Australia	147.237.0.33	idf.il	drop		drop	1
85.65.25.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.106.92.47	Russian Federation	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.56	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
162.213.152.149	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.171	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.106.92.47	Russian Federation	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.247	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
119.9.49.11	Australia	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.90	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.65.25.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.106.92.47	Russian Federation	147.237.0.35	akaws.idf.il	drop		drop	1

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.56.75	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	17
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	2
107.72.162.87	United States	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	Unauthorized URL Access to www.law.idf.il/mobile/templates/getfile/getfile.aspx	Block	1
178.137.86.10	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
84.228.254.72	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
112.95.249.13	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-15612-en/dover.aspx	Block	1
178.137.86.10	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
85.25.197.18	Germany	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
2.51.149.97	United Arab Emirates	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
157.55.39.110	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/default.asp	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/authenticationservice.asmx/getauthuser	Block	1
193.9.245.64	Russian Federation	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
85.25.197.18	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
2.51.149.97	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
157.55.39.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.36	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
89.139.231.58	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
178.137.86.10	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 178.137.86.10	Block	1
82.80.150.191	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.144	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/×'×™×œ×™×• × ××ª	Block	1

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