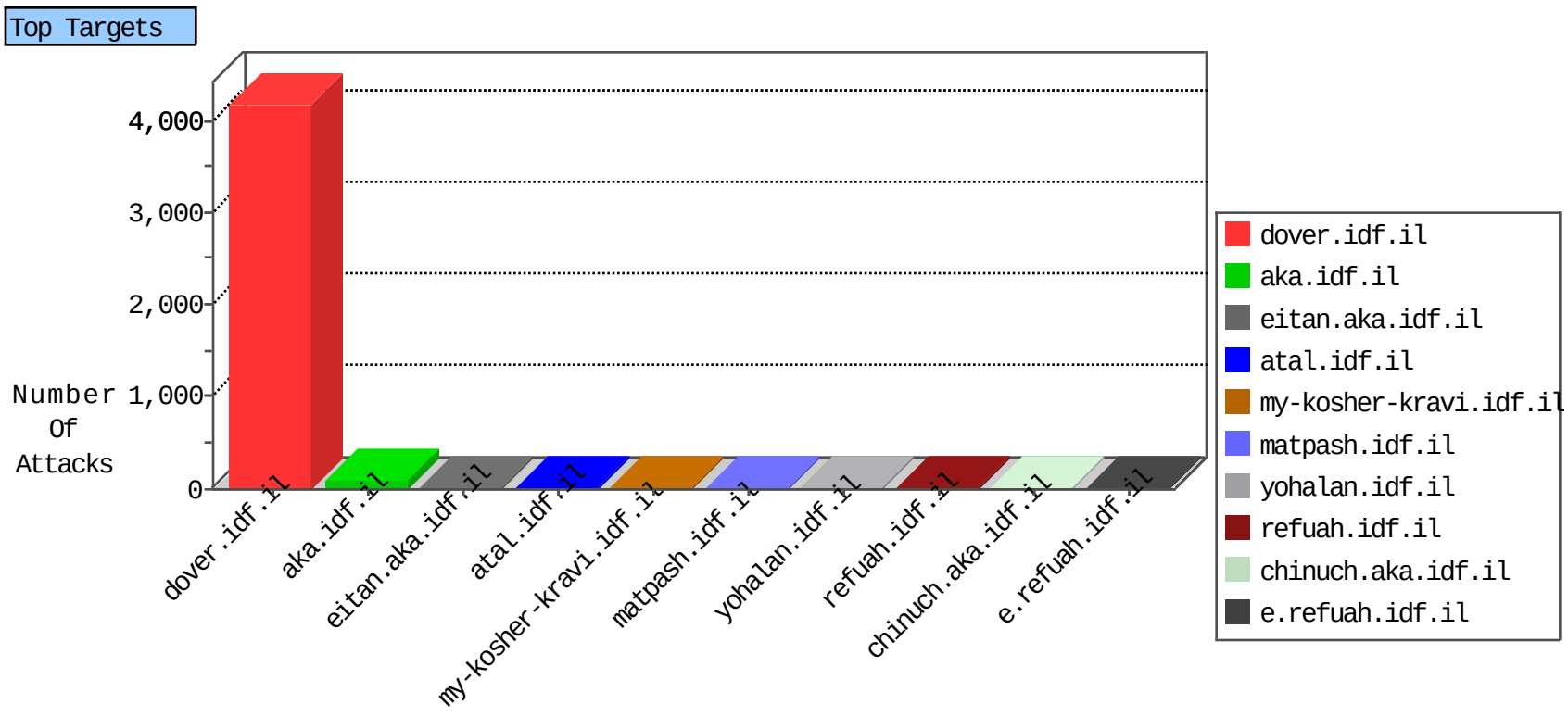
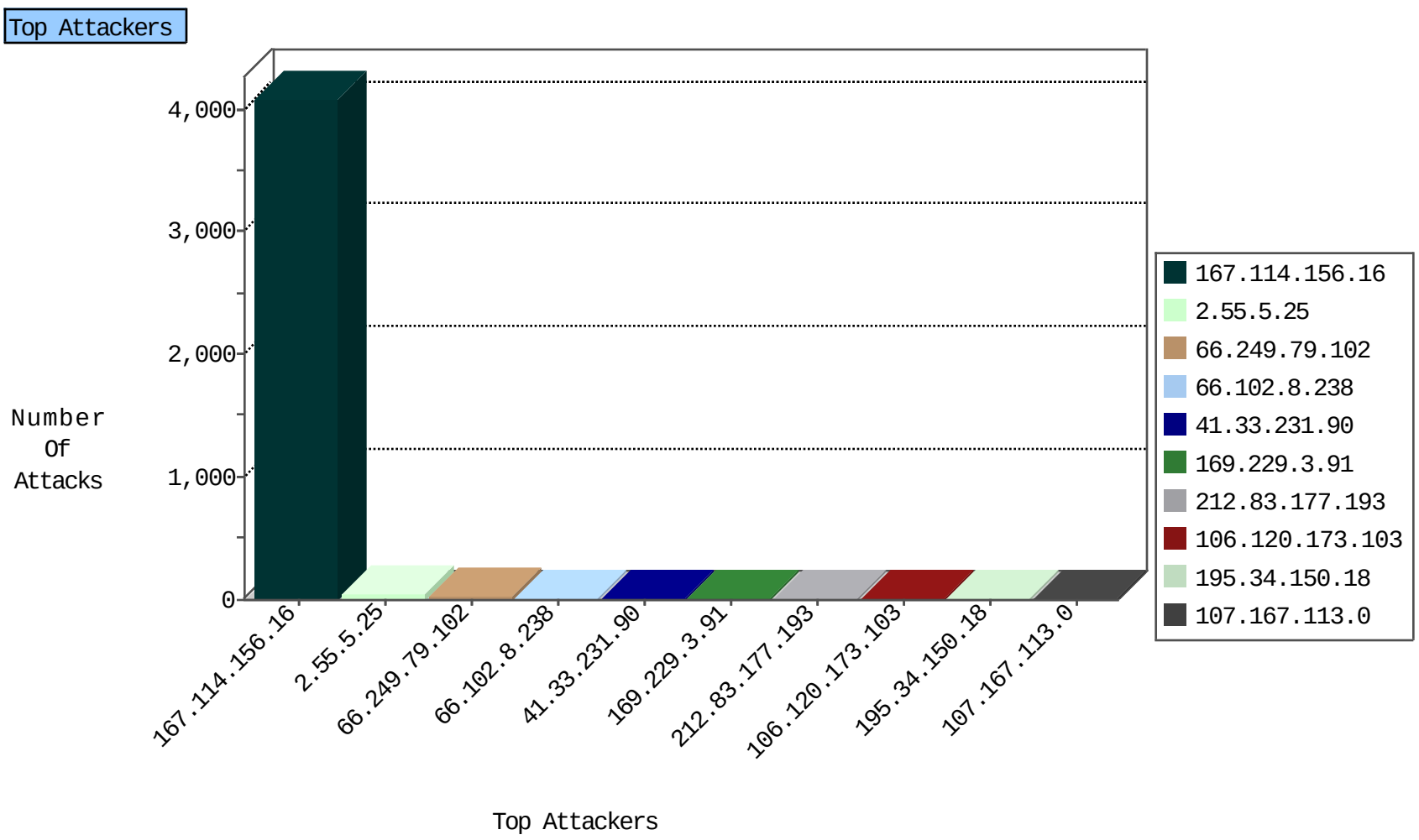
04-18-2016-04:04:05 to 04-18-2016-05:04:05

IDF Under Attack Daily Report





04-18-2016-04:04:05 to 04-18-2016-05:04:05

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	Block_Ip_Web_In	drop	4091
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
159.122.220.135	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
159.122.220.135	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.62	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
159.122.220.135	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

04-18-2016-04:04:05 to 04-18-2016-05:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.83.177.193	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	5
106.120.173.103	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
144.76.61.21	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
151.80.31.182	France	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-18-2016-04:04:05 to 04-18-2016-05:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.79.28	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sA (2)	2
185.112.248.50	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN Potential SSH Scan	1
185.103.252.8	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
40.114.42.13	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
40.84.159.128	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
13.94.233.163	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 4096	1
204.152.218.49	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
13.94.233.163	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -f -sS	1
185.112.248.50	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN Potential SSH Scan	1
185.112.248.50	147.237.77.178	United Kingdom	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
162.144.41.122	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
68.238.163.163	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
40.84.159.128	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
40.84.159.128	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
204.152.218.49	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
13.94.233.163	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 2048	1

04-18-2016-04:04:05 to 04-18-2016-05:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.249.79.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
2.55.5.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
66.102.8.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.55.5.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
2.55.5.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
73.158.219.67	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
107.167.113.0	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.55.5.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
163.172.12.117	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
96.236.210.249	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
207.46.13.37	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.79.10	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
68.180.230.155	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
169.229.3.91	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.200	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.55.5.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.79	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.148.71.133	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
212.143.142.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.201	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.35	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.55.5.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
184.105.139.87	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
168.1.6.35	Australia	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
159.226.95.66	China	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.56	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.111	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.195	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.120	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
159.226.95.66	China	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.101.156.218	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
169.229.3.91	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.196	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
222.73.18.162	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.79	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
162.144.41.122	United States	147.237.76.34	yohalan.idf.il	drop		drop	1

04-18-2016-04:04:05 to 04-18-2016-05:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.214.116.128	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.214.116.128	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.73.235	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip	Block	1
207.46.13.110	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
71.43.100.242	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/).html(	Block	1
163.172.12.117	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9235-he/refuah.aspx	Block	1
85.65.217.64	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip storage/files/	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.83.245	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
197.231.221.211	Liberia	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
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9032-he/refuah.aspx	Block	1
96.236.210.249	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1246-he/atal.aspx	Block	1
198.58.103.102	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
68.180.230.184	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
131.253.25.145	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

04-18-2016-04:04:05 to 04-18-2016-05:04:05