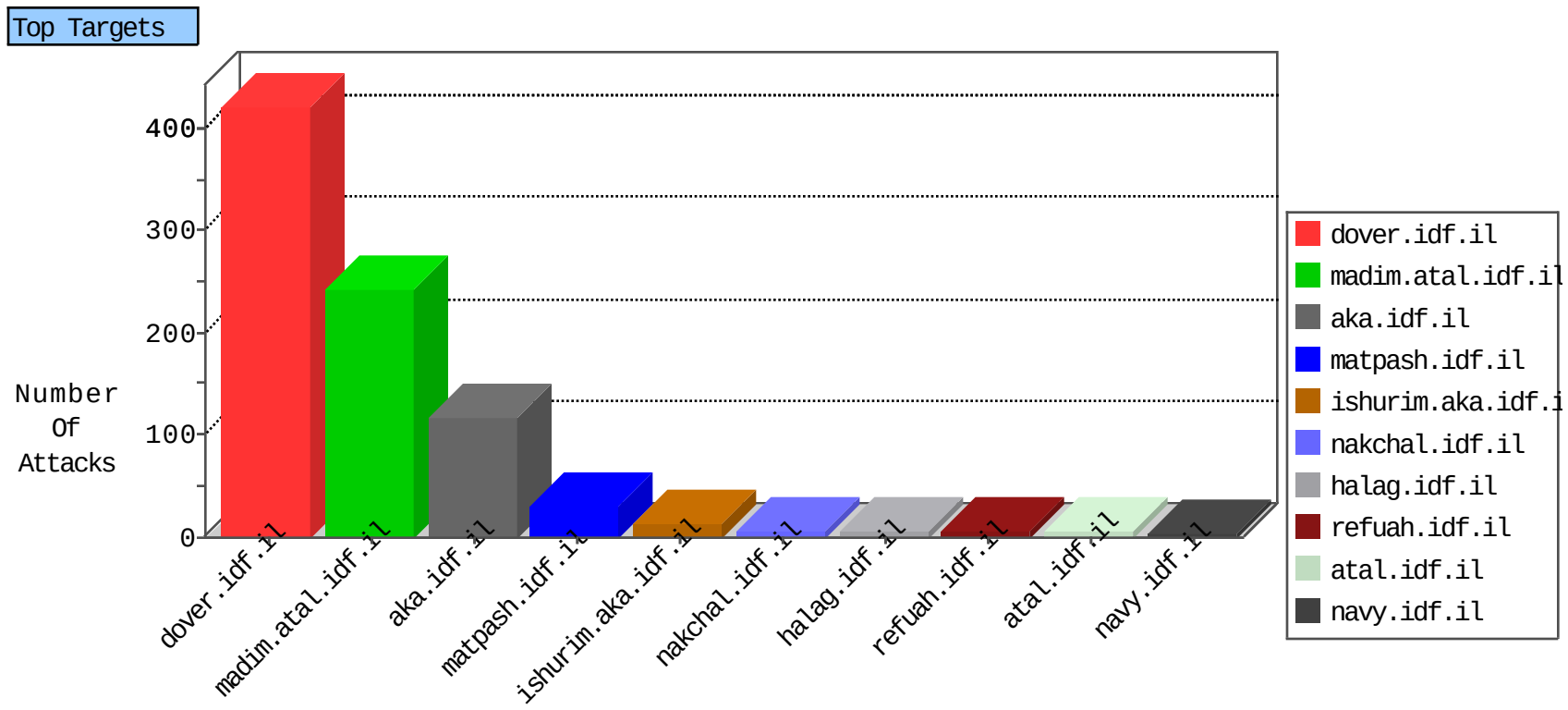
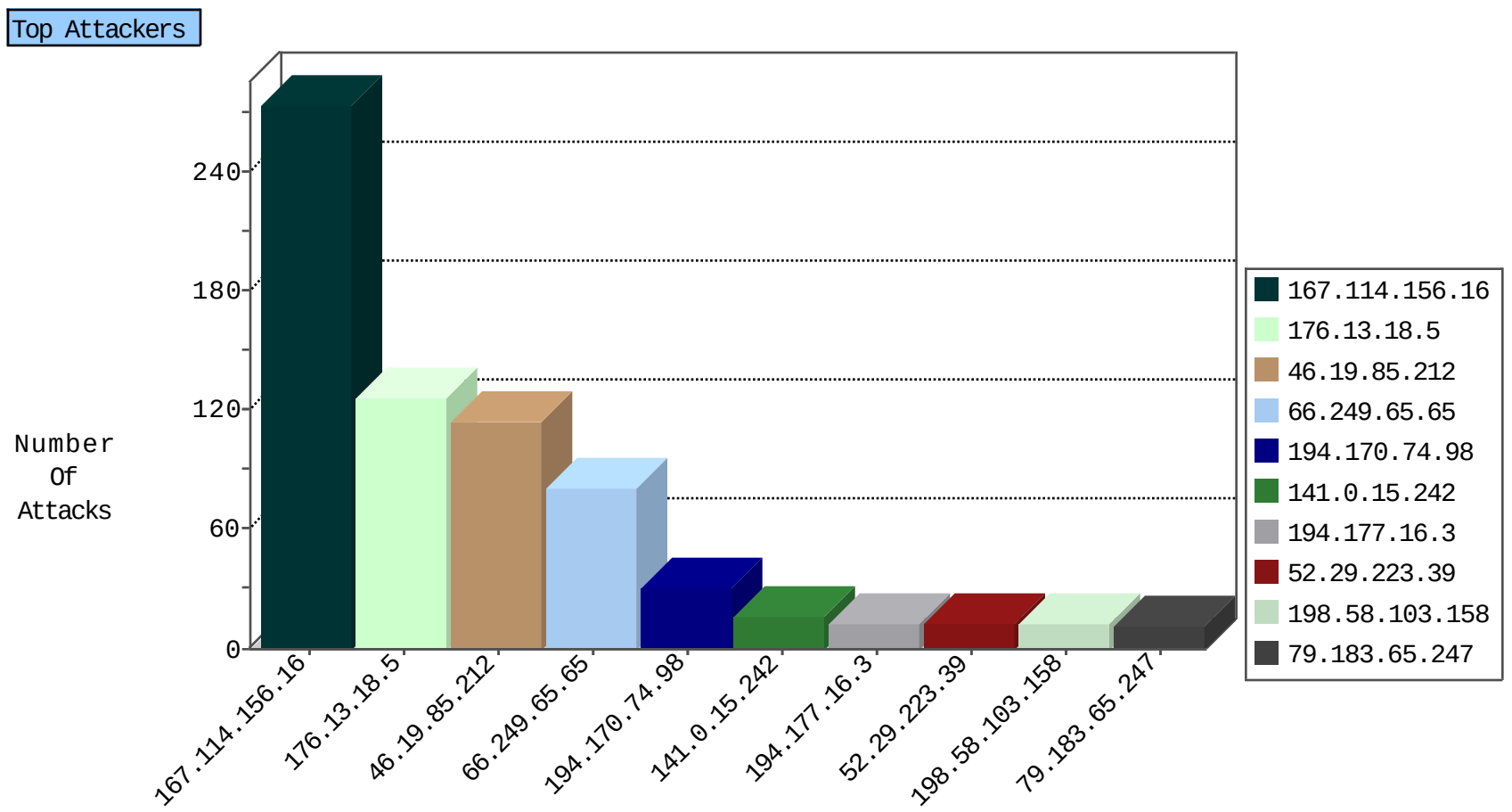
05-04-2016-06:04:09 to 05-04-2016-07:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-04-2016-06:04:09 to 05-04-2016-07:04:09

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	HTTP-POST-Segmented-DoS	dest-reset	11453
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	927
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
41.58.230.86	Nigeria	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
209.126.136.2	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

05-04-2016-06:04:09 to 05-04-2016-07:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-04-2016-06:04:09 to 05-04-2016-07:04:09

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
58.187.229.210	147.237.77.234	Vietnam	halag.idf.il	ET SCAN NMAP -sS window 4096	1
23.246.236.49	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
23.246.236.49	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
208.100.26.228	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.178.142	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.72.166	United States	aka.idf.il	ET DROP Dshield Block Listed Source	1
104.214.25.64	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
104.214.25.64	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
104.128.144.131	147.237.76.31	Canada	nakchal.idf.il	ET SCAN NMAP -f -sS	1
58.187.229.210	147.237.77.234	Vietnam	halag.idf.il	ET SCAN Potential SSH Scan	1
58.187.229.210	147.237.77.234	Vietnam	halag.idf.il	ET SCAN NMAP -sS window 3072	1
23.246.236.49	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
13.92.178.142	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
208.100.26.228	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.178.142	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -f -sS	1
104.214.25.64	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
104.128.144.131	147.237.76.31	Canada	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
76.181.249.213	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1

05-04-2016-06:04:09 to 05-04-2016-07:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
194.170.74.98	United Arab Emirates	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	30
141.0.15.242	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
194.177.16.3	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
198.58.103.158	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
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
100.38.48.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.102.195.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.28.169.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
72.13.86.189	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
82.81.37.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.247	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.137.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.102.195.48	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.73.251	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.79.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.156	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	3
37.26.146.220	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	3
128.242.249.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.51.17.249	United Arab Emirates	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
78.164.126.12	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
213.57.248.132	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.26.148.163	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.53.32.138	Israel	147.237.77.226	www.chamatz.aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
213.57.248.132	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
208.100.26.228	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.248	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.161.9.11	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.84	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
104.128.144.131	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.239	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.116.71.170	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.100	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.100.26.228	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.100	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.186.113.132	Japan	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.5	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	126
46.19.85.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
2.53.178.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.89	Block	2
79.183.65.247	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	1
66.249.93.193	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/homepage/mobile	Block	1
2.51.17.249	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
79.183.65.247	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name úë[[#30]]Üˆ H’ÿ[[#18]]êÆ{GÞÔ[[#3]]°ÄŸ}d[[#26]]Ú#[[#16]]ïšˆ[[#15]] ›æ÷uDD)Æ–"0lš<ë^•¢	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3468.gif	Block	1
79.183.65.247	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at ³–…[[#26]][[#14]]™™[[#1]]¼ðšuÌf~•Ð¸Ñ8.”NEp([[#0]]Ž+µVÆ[[#16]]pji[[#27]]é¦–>[[#24]][[#22]]/`–òk;[[#24]][[#8]]x(c6Š™†[[#7]]¿[[#30]]í¼)8)ÑèLøÁMmjDÇœ¹g	Block	1
66.249.93.196	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on nakhal.idf.il/templates/general/mobile	Block	1
79.183.65.247	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/3397.jpg	Block	1
79.183.65.247	Israel	147.237.72.166	aka.idf.il	NULL Character in Method qo•÷ˆ’çbP[[#0]]4W›•Ì•e×6RR}5¶#~[[#24]]¾[[#25]]÷–bÖ[[#6]]ÂÉ“[[#28]]	Block	1
66.249.93.199	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/general/mobile	Block	1
24.218.80.94	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
184.105.247.195	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
79.183.65.247	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method qo•÷ˆ’çbP[[#0]]4W›•Ì•e×6RR}5¶#~[[#24]]¾[[#25]]÷–bÖ[[#6]]ÂÉ“[[#28]]	Block	1
79.183.65.247	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.183.65.247	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
31.168.145.47	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
217.165.227.153	United Arab Emirates	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile	Block	1
79.183.65.247	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 2	Block	1
66.249.93.193	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on nakhal.idf.il/templates/general/mobile	Block	1
2.51.17.249	United Arab Emirates	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
79.183.65.247	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method qo•÷ˆ’çbP[[#0]]4W›•Ì•e×6RR}5¶#~[[#24]]¾[[#25]]÷–bÖ[[#6]]ÂÉ“[[#28]] in URL	Block	1
79.183.65.247	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1