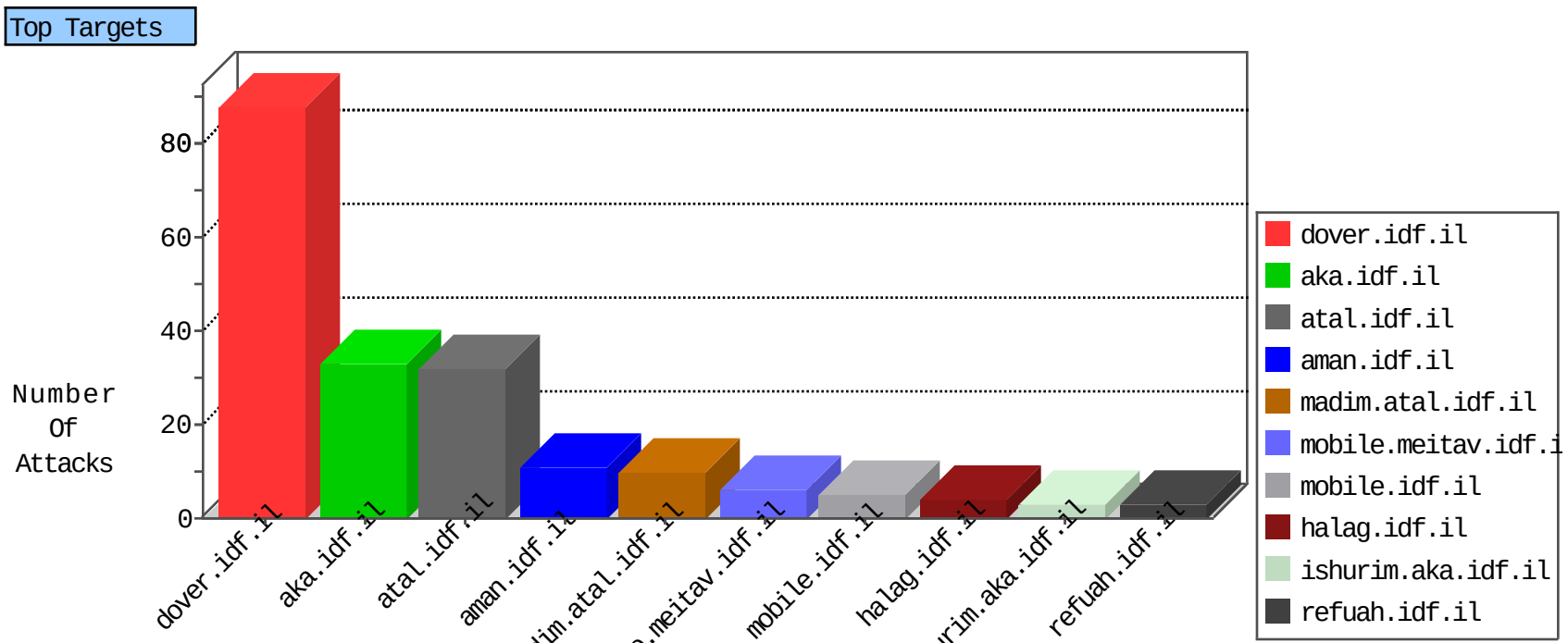
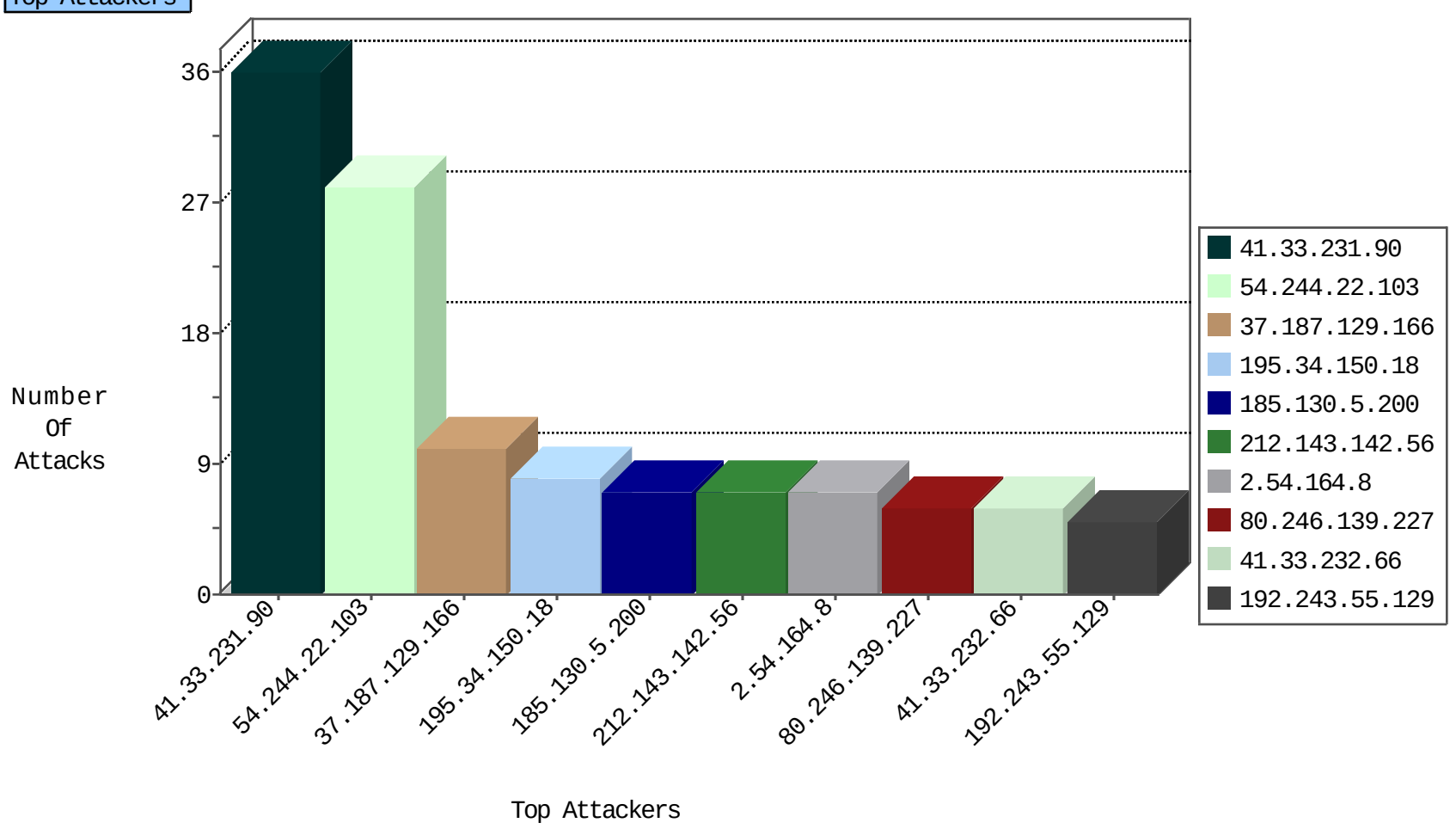
02-07-2016-06:04:04 to 02-07-2016-07:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-07-2016-06:04:04 to 02-07-2016-07:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
111.47.96.116	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	3
120.203.68.110	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
39.128.223.181	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
134.147.203.115	Germany	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
42.2.243.219	Hong Kong	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
192.99.193.12	Canada	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

02-07-2016-06:04:04 to 02-07-2016-07:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-07-2016-06:04:04 to 02-07-2016-07:04:04

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
212.86.219.134	147.237.72.166	Germany	aka.idf.il	Tehila - Perl LWP with fake user agent	4
104.128.144.131	147.237.72.167	Canada	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
185.130.5.200	147.237.77.234		halag.idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.0.33	Austria	idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.200	147.237.76.201		e.atal.idf.il	ET SCAN Potential SSH Scan	1
77.85.35.211	147.237.77.234	Bulgaria	halag.idf.il	ET SCAN NMAP -sS window 4096	1
185.130.5.200	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	1
46.151.52.161	147.237.77.226	Ukraine	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.200	147.237.0.19		madim.atal.idf.il	ET SCAN Potential SSH Scan	1
183.61.143.147	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
115.231.9.148	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
208.67.1.38	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
115.231.9.148	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
95.110.187.71	147.237.0.17	Italy	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.200	147.237.76.202		e.halag.idf.il	ET SCAN Potential SSH Scan	1
91.207.60.30	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.200	147.237.76.177		ncore.idf.il	ET SCAN Potential SSH Scan	1
77.85.35.211	147.237.77.234	Bulgaria	halag.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.200	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
183.82.106.200	147.237.0.200	India	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
115.231.9.148	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
208.67.1.38	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1

02-07-2016-06:04:04 to 02-07-2016-07:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	28
37.187.129.166	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.54.164.8	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.46.39.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.139.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.215.250	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.176.224.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
101.227.59.136	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
2.52.6.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.78.93	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	2
5.22.131.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.100	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
81.169.237.146	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	2
109.186.185.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.147.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.7	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
54.219.106.162	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
104.128.144.131	Canada	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.15	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
81.169.237.146	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
104.130.78.65	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
74.82.47.20	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.227	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
109.186.185.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.227	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
71.246.210.9	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1

02-07-2016-06:04:04 to 02-07-2016-07:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	4
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	4
80.246.139.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.0.197	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
176.13.18.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.18.142	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
173.254.216.67	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
103.255.31.1	Australia	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
207.46.13.115	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list3.htm	Block	1
79.176.149.162	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mce_src=	Block	1
157.55.39.100	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/military-police/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
207.46.13.142	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
178.32.53.53	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.179.118.132	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$20 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.65.188	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1242-he/atal.aspx	Block	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/pratim/pirteytkufa/?docid=37891	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
216.245.218.190	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
184.95.47.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 184.95.47.166	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
194.187.168.216	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;sideScroll in www.aka.idf.il/giyus/general/	None	1
207.46.13.34	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/size220x0/sip_storage	Block	1
73.15.105.163	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1

02-07-2016-06:04:04 to 02-07-2016-07:04:04