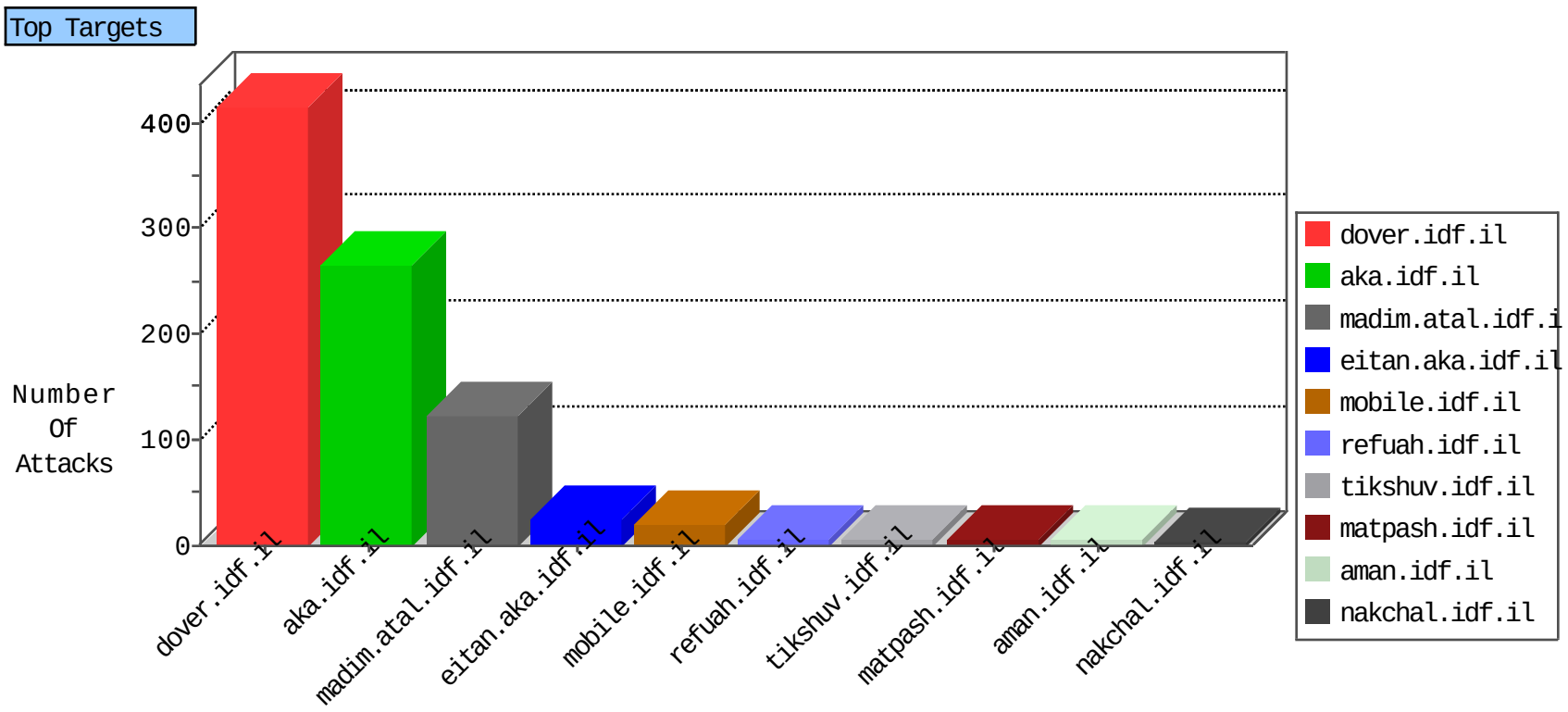
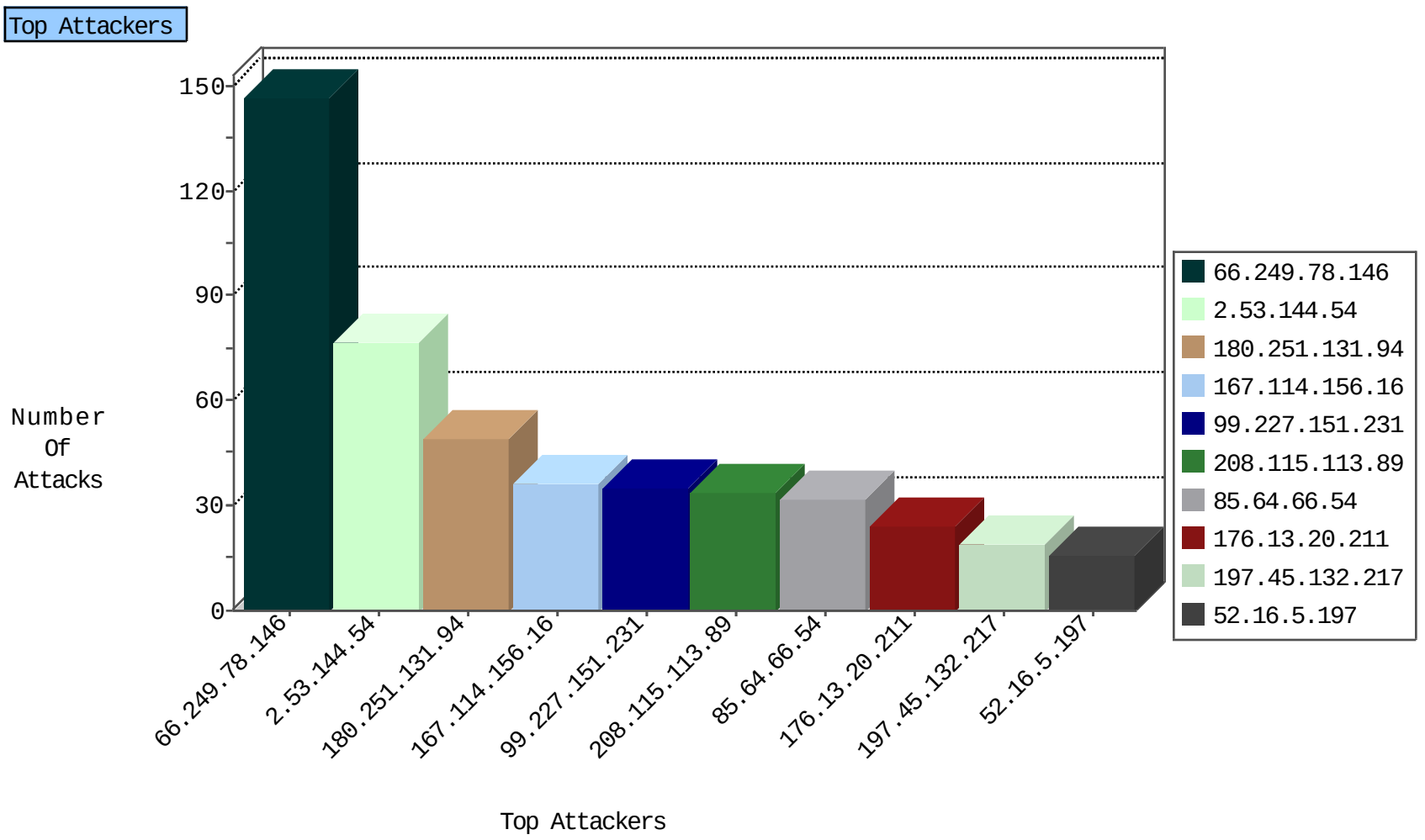
05-03-2016-07:04:01 to 05-03-2016-08:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



05-03-2016-07:04:01 to 05-03-2016-08:04:01

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	1792
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	520
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
71.6.216.50	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
71.6.216.51	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.130	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

05-03-2016-07:04:01 to 05-03-2016-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

05-03-2016-07:04:01 to 05-03-2016-08:04:01

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
91.201.236.155	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
220.249.194.151	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.140.23	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
120.203.215.106	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
212.129.15.245	147.237.76.176	France	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
189.219.42.185	147.237.76.38	Mexico	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.140.23	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

05-03-2016-07:04:01 to 05-03-2016-08:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	147
180.251.131.94	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
99.227.151.231	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
85.64.66.54	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
176.13.20.211	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	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	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.254.65.232	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.146.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
92.241.53.140	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.178.13.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.64.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
62.78.243.55	Finland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
103.55.110.129	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.114.91.245	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.64.146.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.179.36.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.152.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.147.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.202.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.106.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.146.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.198.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
194.187.168.223	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.33.123.23	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.64.103	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

05-03-2016-07:04:01 to 05-03-2016-08:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.144.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
2.53.171.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
109.253.226.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
188.116.33.163	Poland	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 188.116.33.163	Block	5
176.13.23.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.53.41.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.4.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.116.177.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
131.253.25.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.218	Israel	147.237.76.31	nakchal.idf.il	Malformed URL	Block	1
195.154.199.235	France	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1613-15489-he/dover.aspx	Block	1
106.186.113.132	Japan	147.237.77.235	sviva.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.218	Israel	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method endToFriend/SendToFriend.aspx?&l=he&f=1072 in URL	Block	1
195.154.199.235	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
2.53.191.45	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
188.116.33.163	Poland	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
213.254.241.5	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$btnSearch in www.aka.idf.il/main/sachar/default.aspx	None	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8896-he/refuah.aspx	Block	1
37.26.147.200	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/general/mobile	Block	1
62.90.255.56	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 62.90.255.56	Block	1
216.218.206.66	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
180.251.131.94	Indonesia	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
79.178.175.178	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.19.85.218	Israel	147.237.76.31	nakchal.idf.il	Distributed Abnormally Long Request	Block	1
164.138.123.229	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
62.90.255.56	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	1
185.32.179.42	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.182.130.43	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1

05-03-2016-07:04:01 to 05-03-2016-08:04:01