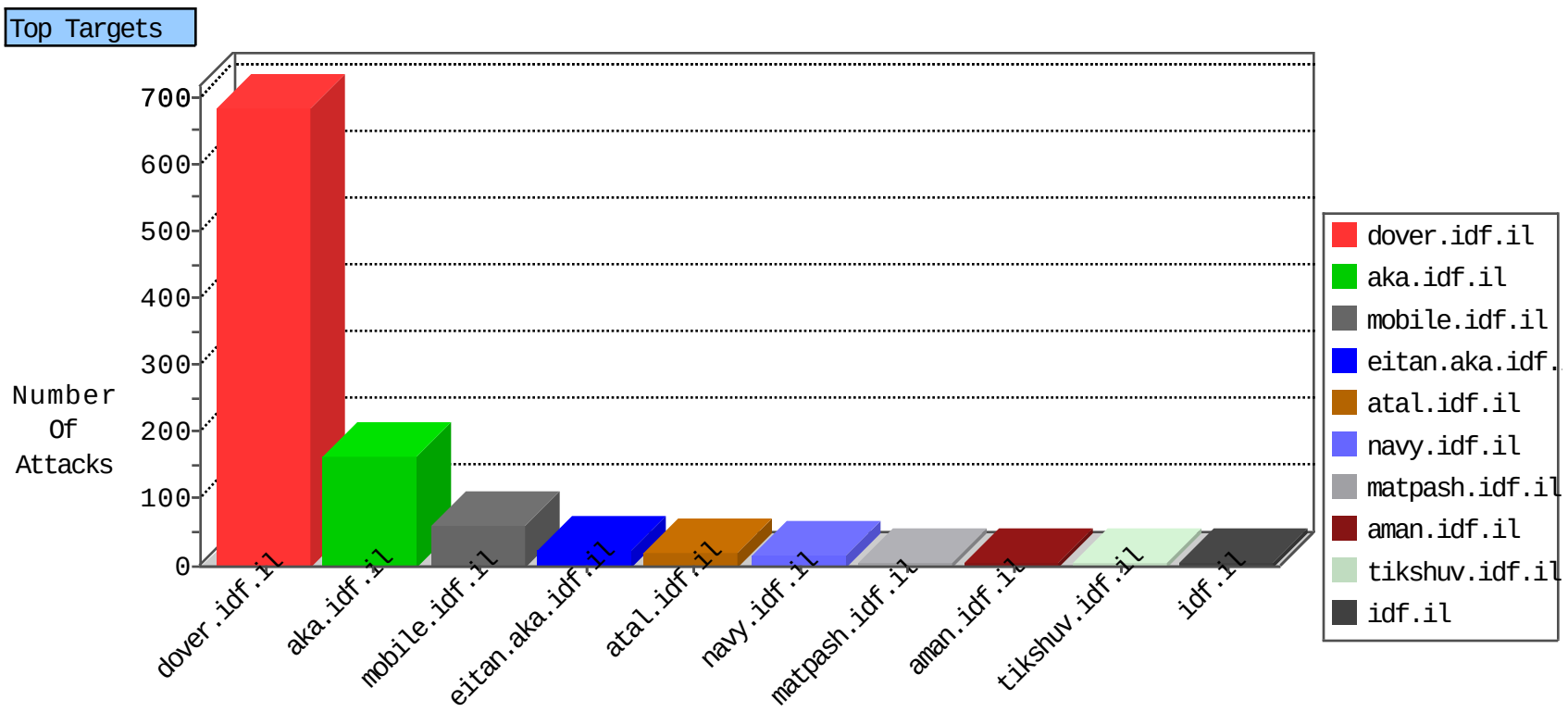
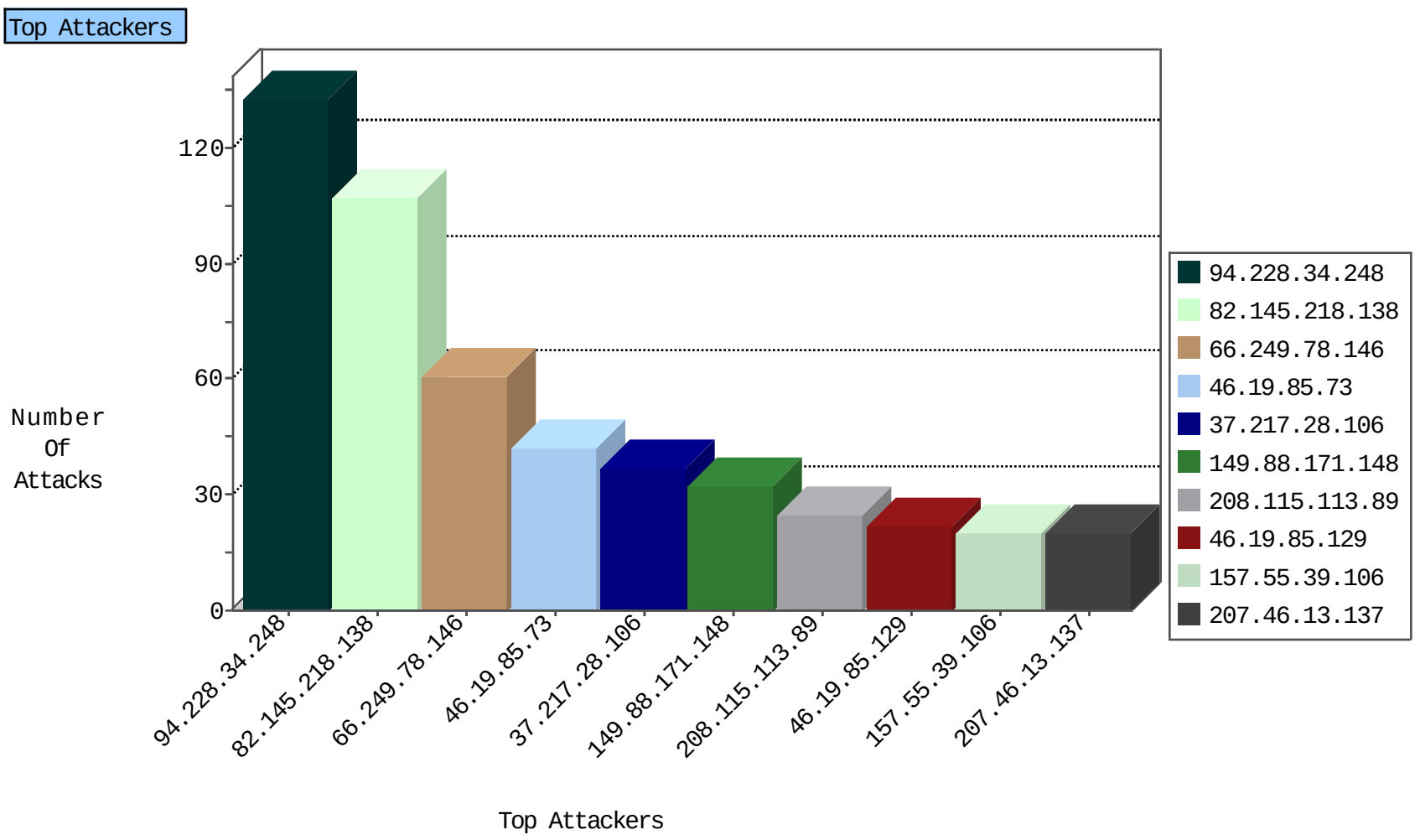
04-29-2016-01:04:29 to 04-29-2016-02:04:29

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-29-2016-01:04:29 to 04-29-2016-02:04:29

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	5
71.6.165.200	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

04-29-2016-01:04:29 to 04-29-2016-02:04:29

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-29-2016-01:04:29 to 04-29-2016-02:04:29

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.186	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.159	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
119.10.114.32	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
89.248.167.131	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
189.122.22.172	147.237.8.27	Brazil	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
119.10.114.32	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
104.219.238.10	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential SSH Scan	1
66.240.213.93	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.211	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
119.10.114.32	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1

04-29-2016-01:04:29 to 04-29-2016-02:04:29

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	133
82.145.218.138	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	107
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
37.217.28.106	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
46.19.85.73	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
149.88.171.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
176.7.53.111	Germany	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
169.199.19.136	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
203.133.169.234	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
207.46.13.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.0.101.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.88.171.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
24.87.135.15	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
80.246.130.186	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.70.123.13	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.129	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.129	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
73.171.202.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.109.73.190	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
65.55.210.107	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
200.229.44.1	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.120.154.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.230.86.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
86.108.98.31	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4

04-29-2016-01:04:29 to 04-29-2016-02:04:29

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.92.190	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	11
46.19.85.73	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.250	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.160.147.131	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/images/1.he/infocenteritem/	Block	1
52.87.211.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
213.57.228.26	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus	Block	1
141.212.122.161	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
40.77.167.96	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wut	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/71556.pdf	Block	1
79.182.42.55	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
203.133.170.171	Korea, Republic of	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
66.249.66.182	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
46.120.142.196	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl63 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
213.8.204.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1

04-29-2016-01:04:29 to 04-29-2016-02:04:29