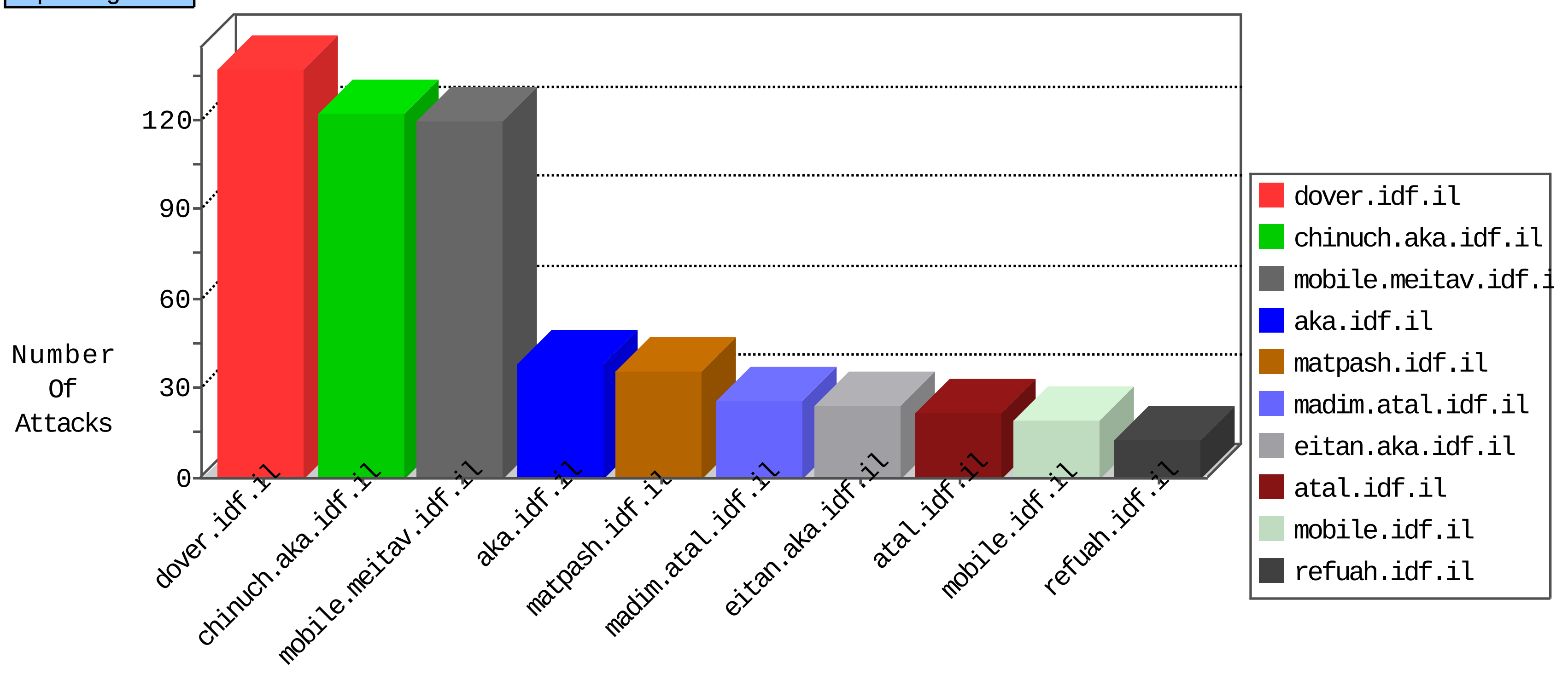
09-25-2016-01:05:44 to 09-25-2016-02:05:44

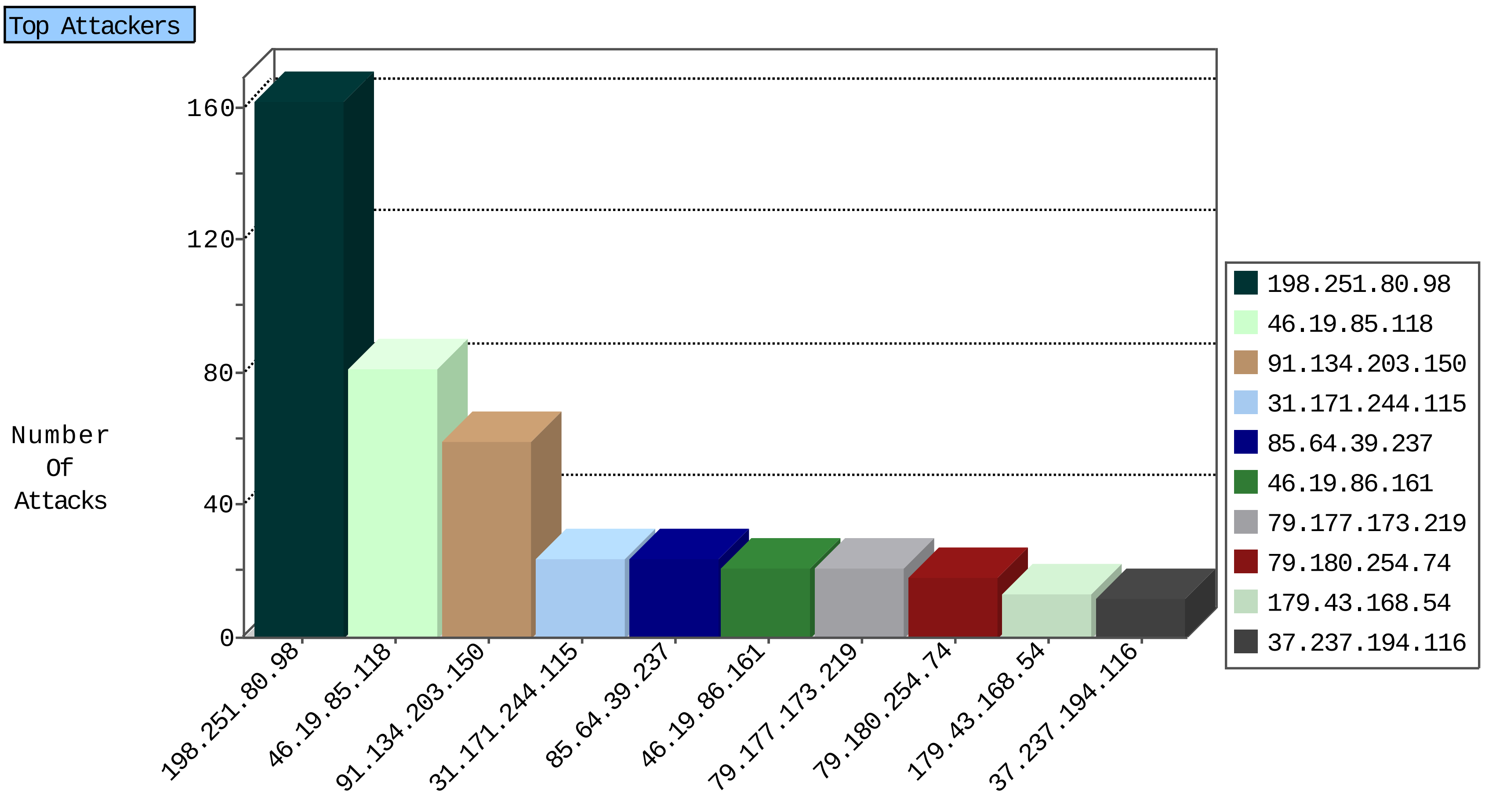
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-25-2016-01:05:44 to 09-25-2016-02:05:44

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.236.86.32	Netherlands	147.237.76.31	nakchal.idf.il	Black List	drop	1
82.118.233.249	Bulgaria	147.237.76.86	navy.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
82.118.233.249	Bulgaria	147.237.76.196	e.sviva.idf.il	Black List	drop	1
82.118.233.249	Bulgaria	147.237.76.202	e.halag.idf.il	Black List	drop	1
31.204.128.22	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

09-25-2016-01:05:44 to 09-25-2016-02:05:44

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-25-2016-01:05:44 to 09-25-2016-02:05:44

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.152.83.12	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
209.95.50.84	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
180.213.5.205	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
116.77.72.71	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
91.234.226.105	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
83.103.175.25	147.237.77.19	Romania	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.69.228	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
49.205.132.204	147.237.76.148	India	gqcenter.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.213.5.205	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
139.162.187.89	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
116.77.72.71	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
86.122.146.180	147.237.72.167	Romania	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.246.133.101	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
5.15.194.115	147.237.76.199	Romania	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

09-25-2016-01:05:44 to 09-25-2016-02:05:44

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
31.171.244.115	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
85.64.39.237	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	22
46.19.85.118	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	19
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	19
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	18
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	18
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
46.19.85.118	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
37.237.194.116	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
91.134.203.150	Bulgaria	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	7
91.134.203.150	Bulgaria	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	7
45.59.183.112	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.86.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
91.134.203.150	Bulgaria	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
79.180.254.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
91.134.203.150	Bulgaria	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	6
79.180.254.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
106.39.60.189	China	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
91.134.203.150	Bulgaria	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.154.49.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.134.203.150	Bulgaria	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
91.134.203.150	Bulgaria	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
79.180.254.74	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
91.134.203.150	Bulgaria	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
84.229.22.14	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
91.134.203.150	Bulgaria	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
91.134.203.150	Bulgaria	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.86.161	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.53.3.238	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.161	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
84.229.22.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
80.246.133.101	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.102.9.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.50.5	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.25	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.50.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.187.87	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
46.19.86.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
179.43.168.54	Switzerland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.173.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	3
46.19.85.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.12.195.33	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
2.53.151.100	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.217	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/captcha.ashx	Block	1
66.249.69.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/assetlinks.json	Block	1
31.154.81.69	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
79.179.50.162	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.242	Israel	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.law.idf.il/163-6639-he/patzar.aspx	Block	1
31.154.49.161	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
166.216.157.75	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
40.142.24.150	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/index.php	Block	1
31.154.81.0	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
207.46.13.156	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/captcha.ashx	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21518-he/idfgdover.aspx	Block	1
85.64.243.143	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.69.229	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.229	Block	1
31.154.81.0	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
77.237.138.202	Czech Republic	147.237.77.170	maarachot.idf.il	Unauthorized Method HEAD for /	Block	1
54.162.124.221	United States	147.237.72.156	aman.idf.il	Unauthorized Method HEAD for 147.237.72.156/	Block	1
109.65.187.87	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.69.229	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/apple-app-site-association	Block	1
31.154.81.69	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
66.249.66.18	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/112981.pdf	Block	1

09-25-2016-01:05:44 to 09-25-2016-02:05:44