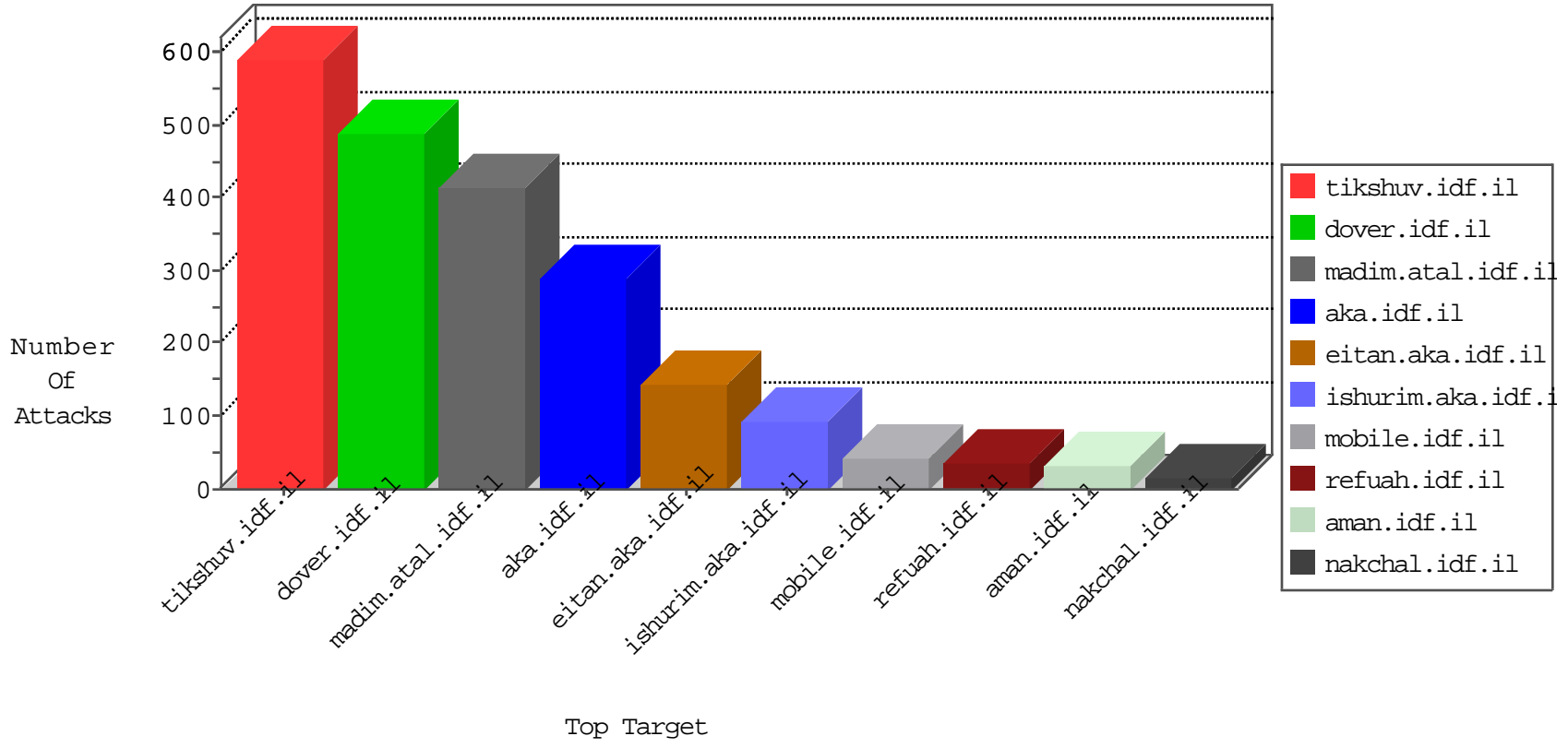


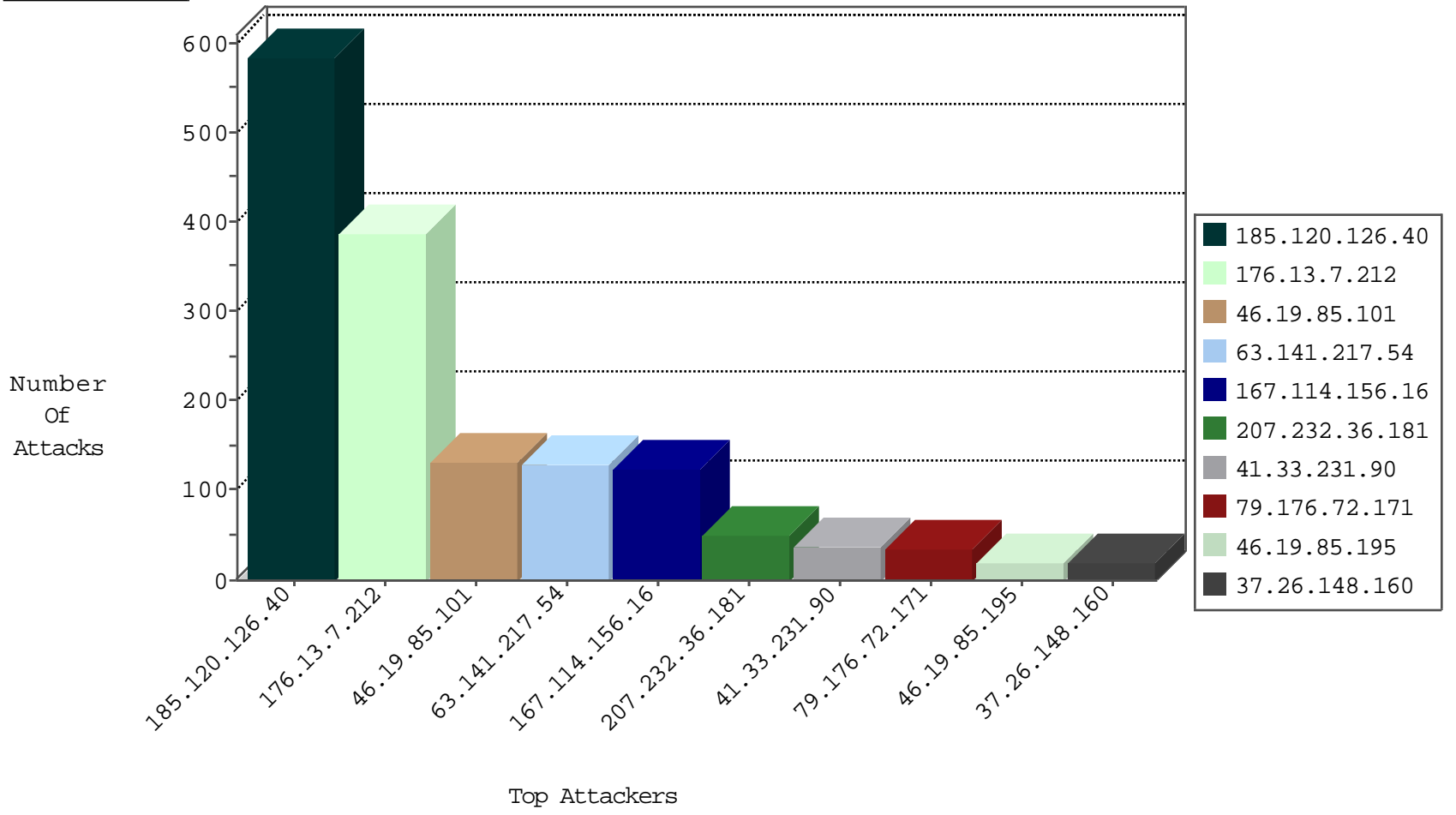
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	7628
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1816
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	894
207.232.36.181	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	589
63.141.217.54	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	23
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	5
31.168.133.226	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
183.60.48.25	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
151.217.178.35		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

12-29-2015-08:04:00 to 12-29-2015-09:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
82.80.25.221	147.237.77.216	Israel	dover.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	2
82.80.198.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
197.45.153.74	147.237.77.179	Egypt	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
82.80.25.221	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache SSI error page cross-site scripting	1
59.45.79.117	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.36	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
108.30.83.8	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -f -sS	1
37.26.148.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
92.61.225.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.77.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.219.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.162.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
197.45.153.74	147.237.77.179	Egypt	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
79.176.131.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.61.109.189	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
176.13.15.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
108.30.83.8	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
46.120.80.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.143.14.247	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.148.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.165.96	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.42.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.204.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.101	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	132
63.141.217.54	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	119
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.176.72.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
37.26.148.160	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
46.19.85.89	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.85.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.52.161.19	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
217.194.199.124	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
66.249.93.140	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	12
82.145.209.99	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
79.176.72.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
62.0.200.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
66.249.78.37	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.117.170.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
176.13.15.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.116.190.206	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.54.131.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
77.125.96.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.91	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
149.78.63.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.173	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.116.96.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.249	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.17	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.249	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
81.218.123.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
189.236.69.8	Mexico	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.117.136.103	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.3.240	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.93.192	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.0.200.160	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
81.218.123.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
176.12.143.159	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.86.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.252	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.17.69	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.97.12	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

