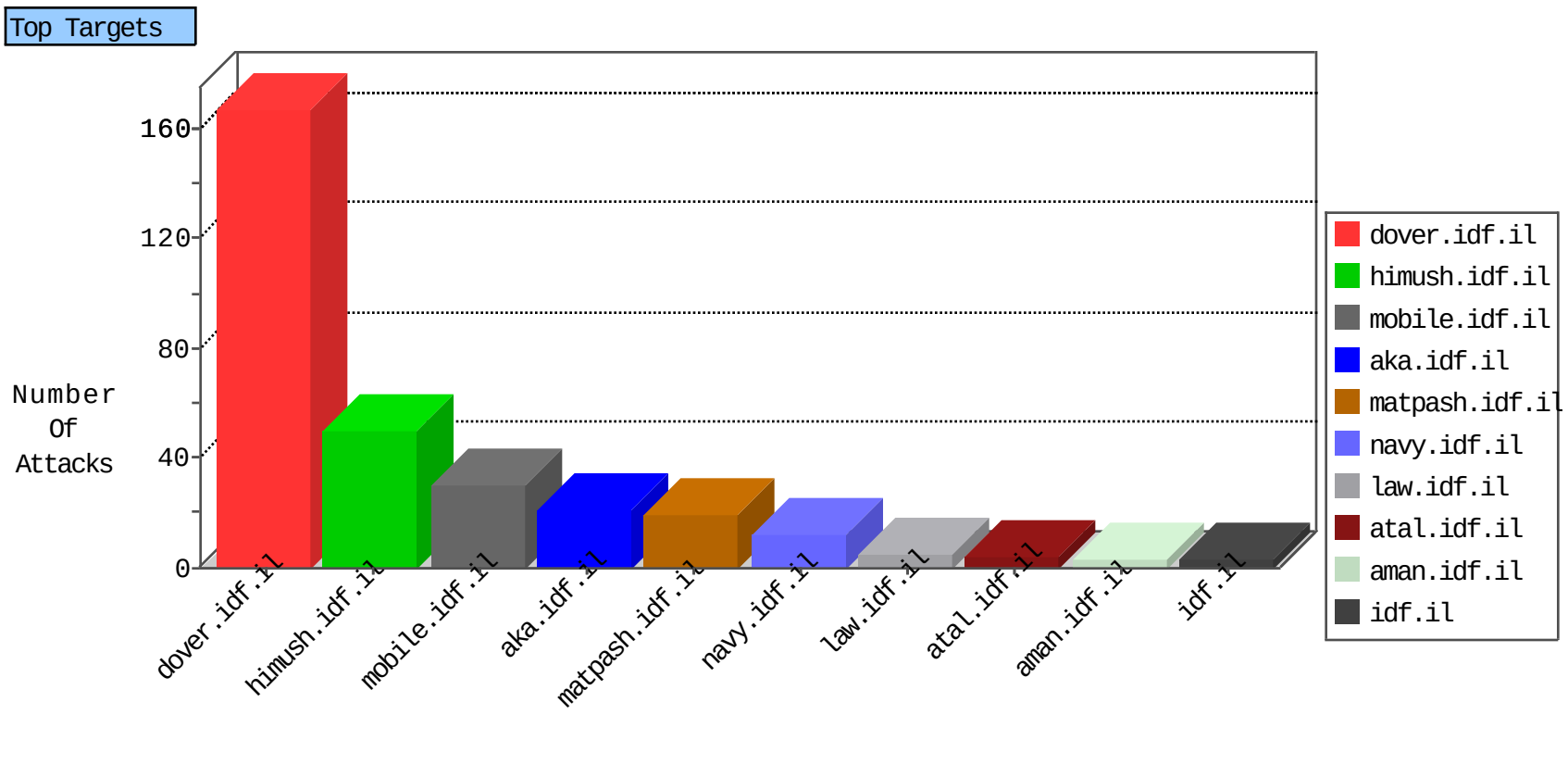
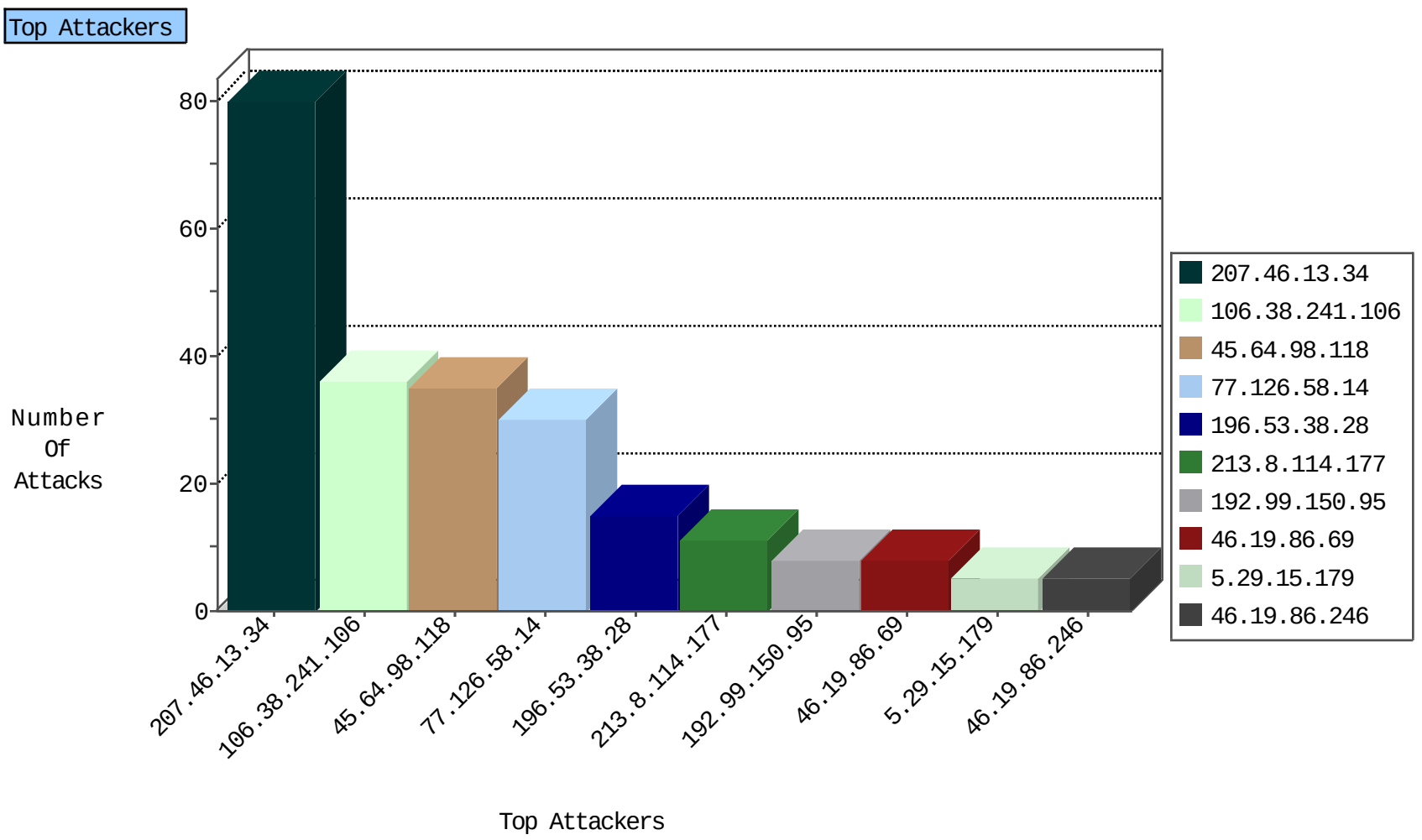
10-03-2016-08:04:09 to 10-03-2016-09:04:09

IDF Under Attack Daily Report





10-03-2016-08:04:09 to 10-03-2016-09:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
200.236.211.185	Brazil	147.237.77.226	www.chamatz.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
180.97.106.162	China	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
200.236.211.185	Brazil	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
200.236.211.185	Brazil	147.237.77.205	prisha.idf.il	JLM_Purple_Con_Limit_Http	drop	1
93.174.94.235	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

10-03-2016-08:04:09 to 10-03-2016-09:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	32
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

10-03-2016-08:04:09 to 10-03-2016-09:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.150.174.201	147.237.77.216	Spain	dover.idf.il	Xenu Link Sleuth User Agent	2
124.188.203.106	147.237.72.166	Australia	aka.idf.il	ET SCAN Potential SSH Scan	2
61.221.69.222	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
23.239.31.132	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
223.100.131.121	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
211.149.222.5	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
203.106.184.157	147.237.76.147	Malaysia	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
183.129.160.229	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
111.68.107.43	147.237.76.198	Pakistan	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
61.221.69.222	147.237.0.33	Taiwan	idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
211.149.222.5	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.222.5	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
208.80.155.222	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
192.223.94.47	147.237.72.156	Bolivia	aman.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.102.48.194	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1

10-03-2016-08:04:09 to 10-03-2016-09:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	80
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
196.53.38.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
45.64.98.118	Indonesia	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
45.64.98.118	Indonesia	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	7
45.64.98.118	Indonesia	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
45.64.98.118	Indonesia	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
213.8.114.177	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
45.64.98.118	Indonesia	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
5.29.15.179	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
213.8.114.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.86.99	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.95.251.156	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
74.85.206.41	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
79.181.193.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.183.163.6	Italy	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.246	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
82.193.127.15	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
106.38.241.106	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.29.50.221	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.117	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.126.91.120	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
157.55.39.145	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.99.150.95	Canada	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
46.19.86.236	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.106.46.74	Palestinian Territory, Occupied	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
109.253.223.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.98	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.99.150.95	Canada	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
185.120.125.150	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.86.71	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
164.132.202.49	Italy	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.38.241.106	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
75.85.98.19	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
192.99.150.95	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
184.105.139.116	United States	147.237.0.33	idf.il	drop		drop	1
46.19.86.69	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
110.78.157.134	Thailand	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
74.82.47.15	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.120.126.27	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
164.132.202.49	Italy	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
192.99.150.95	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.226	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.69	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

10-03-2016-08:04:09 to 10-03-2016-09:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.240.225	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.13.240.225	Block	1
80.246.136.110	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 80.246.136.110 (Open Mode)	None	1
139.162.13.205	Singapore	147.237.77.226	www.chamatz.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.120.74.53	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
176.13.240.225	Israel	147.237.72.166	aka.idf.il	Unknown Parameter asm in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
80.246.136.110	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.81	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
49.228.231.245	Thailand	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
212.46.65.67	Italy	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.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
157.55.39.104	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
71.6.165.200	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1367-8653-he/atal.aspx	Block	1
110.171.186.212	Thailand	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
176.13.20.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
74.6.254.105	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/17468.jpg	Block	1
139.162.13.205	Singapore	147.237.77.226	www.chamatz.aka.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1

10-03-2016-08:04:09 to 10-03-2016-09:04:09