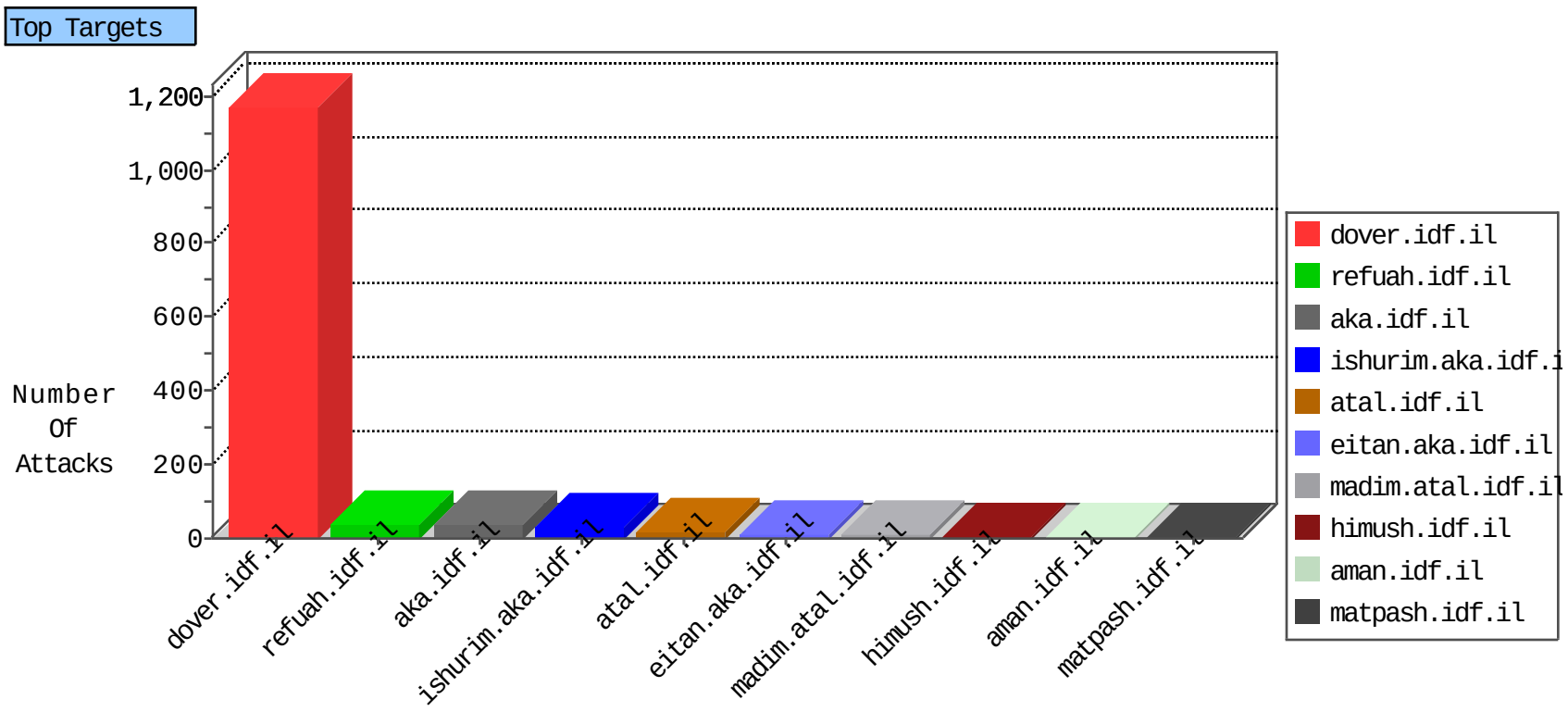
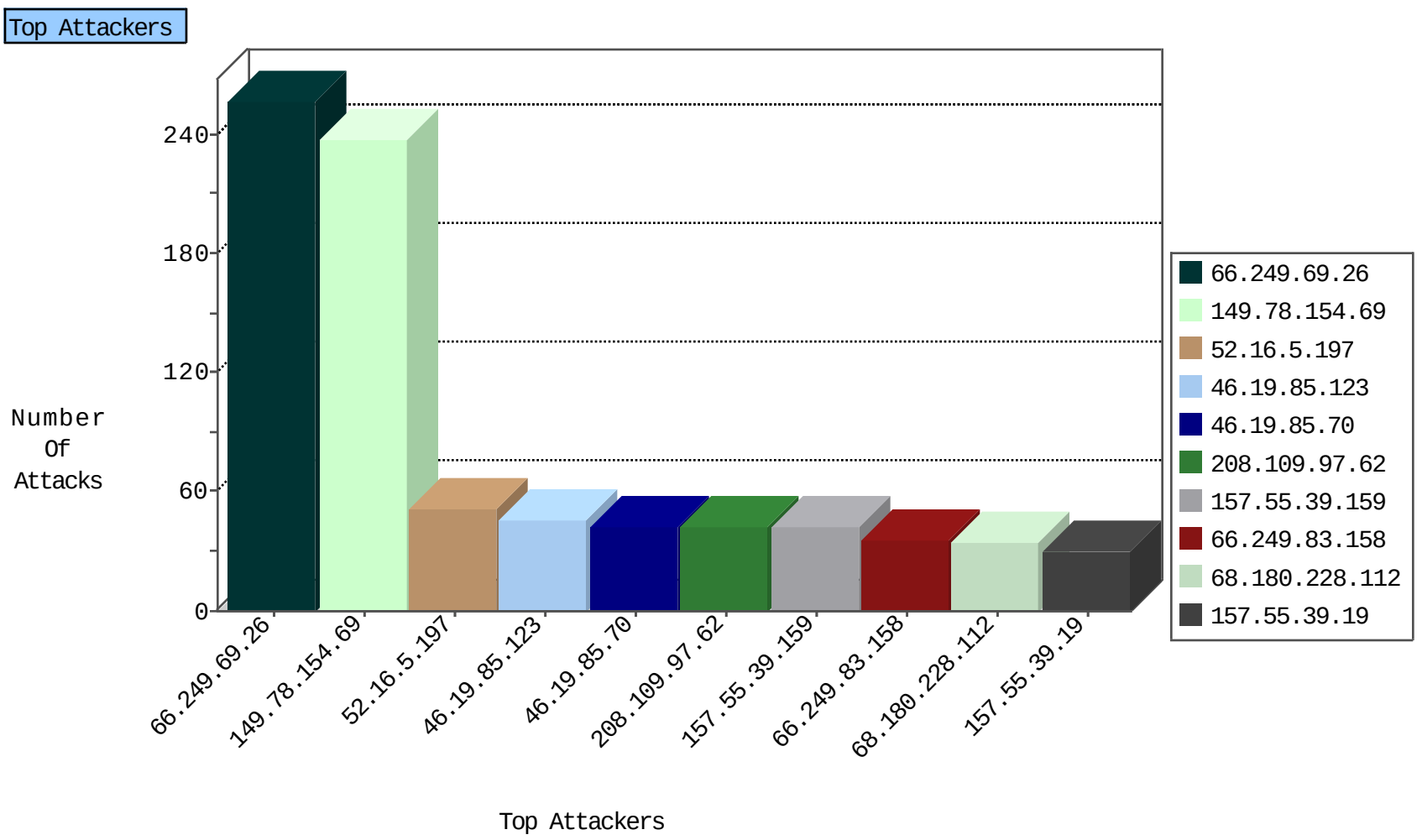
02-14-2016-02:04:00 to 02-14-2016-03:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-14-2016-02:04:00 to 02-14-2016-03:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
115.230.124.164	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
89.248.174.4	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

02-14-2016-02:04:00 to 02-14-2016-03:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
155.94.254.143	United States	147.237.77.234	halag.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1

02-14-2016-02:04:00 to 02-14-2016-03:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
222.186.130.223	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
208.80.155.224	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
93.113.125.11	147.237.76.197	Romania	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.237.52.112	147.237.0.33	Poland	idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 2048	1
222.186.130.223	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
183.61.143.147	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
91.237.52.112	147.237.77.216	Poland	dover.idf.il	ET SCAN Potential SSH Scan	1
80.82.79.104	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -f -sS	1

02-14-2016-02:04:00 to 02-14-2016-03:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.123	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
46.19.85.70	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.85.70	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	15
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
185.3.147.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.130	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
95.35.131.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
208.109.97.62	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.70	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.16.160	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.157.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.160.5	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
176.13.12.87	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.253.209.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
83.130.121.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
176.13.12.87	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
205.209.74.201	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
109.253.195.81	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
83.130.121.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
54.162.16.100	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
109.253.195.81	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.230	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
156.197.87.107		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
68.105.113.80	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.123	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
134.170.12.194	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
93.113.125.11	Romania	147.237.76.197	e.himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
71.59.194.91	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.13.12.87	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
134.170.12.194	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
208.80.155.224	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
176.13.12.87	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.123	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
83.130.121.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
71.59.194.91	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
195.62.53.168	Russian Federation	147.237.0.35	akaws.idf.il	drop		drop	1
141.8.183.11	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.85.209	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	255
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	238
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	51
157.55.39.159	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
66.249.83.158	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	36
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	36
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	33
157.55.39.19	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
40.77.167.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
89.139.146.112	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
80.246.130.168	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
45.35.64.142		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
95.35.131.195	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
2.54.149.1	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
70.133.148.219	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
2.54.26.214	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
77.126.92.47	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
5.28.142.29	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
37.26.149.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
213.57.138.24	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
62.0.102.190	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
207.232.12.81	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
213.8.204.25	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
77.125.116.214	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
46.120.250.184	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
78.225.154.157	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
209.133.111.211	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
79.177.218.68	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
205.203.135.1	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
66.249.83.160	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
66.249.91.14	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
107.170.119.178	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
185.24.207.48	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
176.13.12.87	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
2.54.19.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.171.64	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
176.13.15.236	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
87.68.60.203	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
79.176.42.29	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
192.198.151.45	Europe	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2

02-14-2016-02:04:00 to 02-14-2016-03:04:00