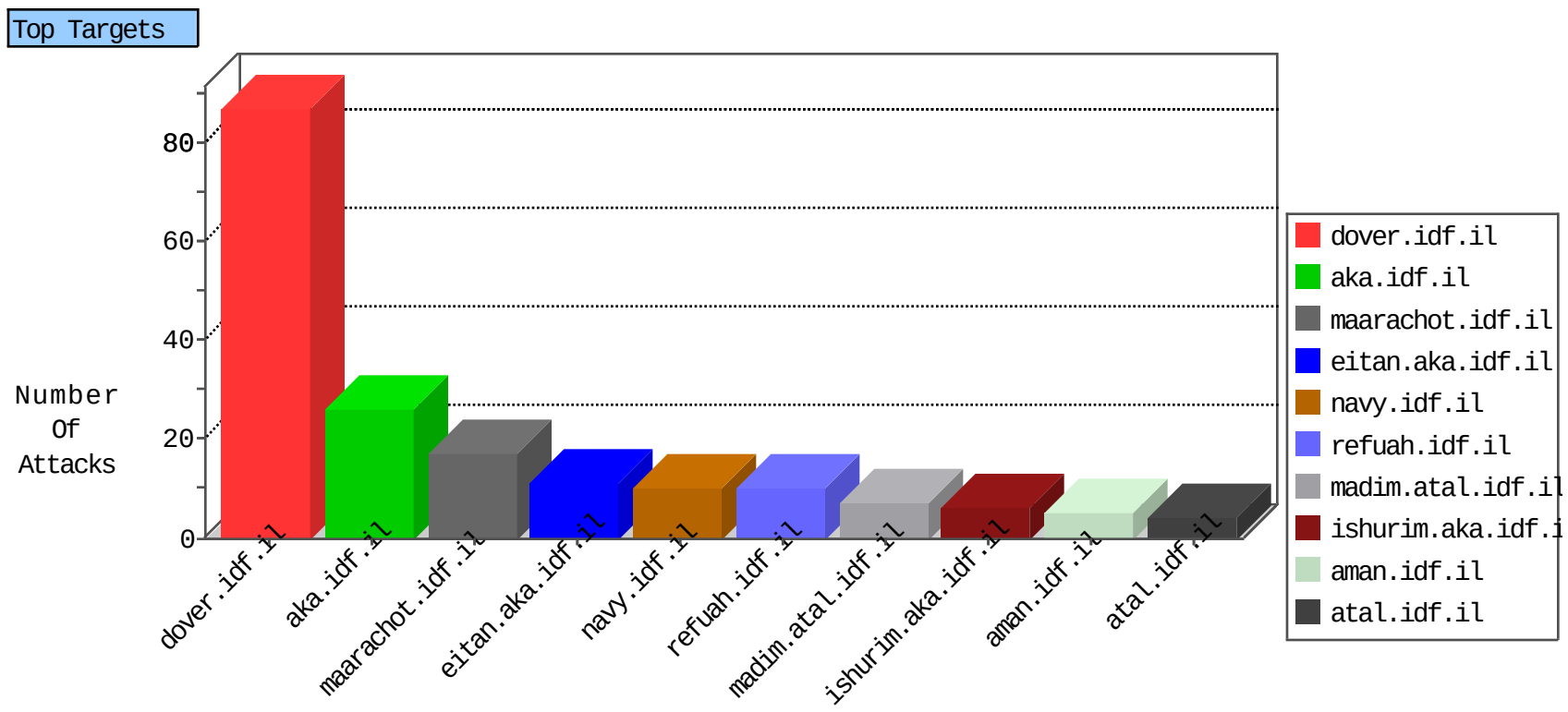
10-04-2016-02:04:06 to 10-04-2016-03:04:06

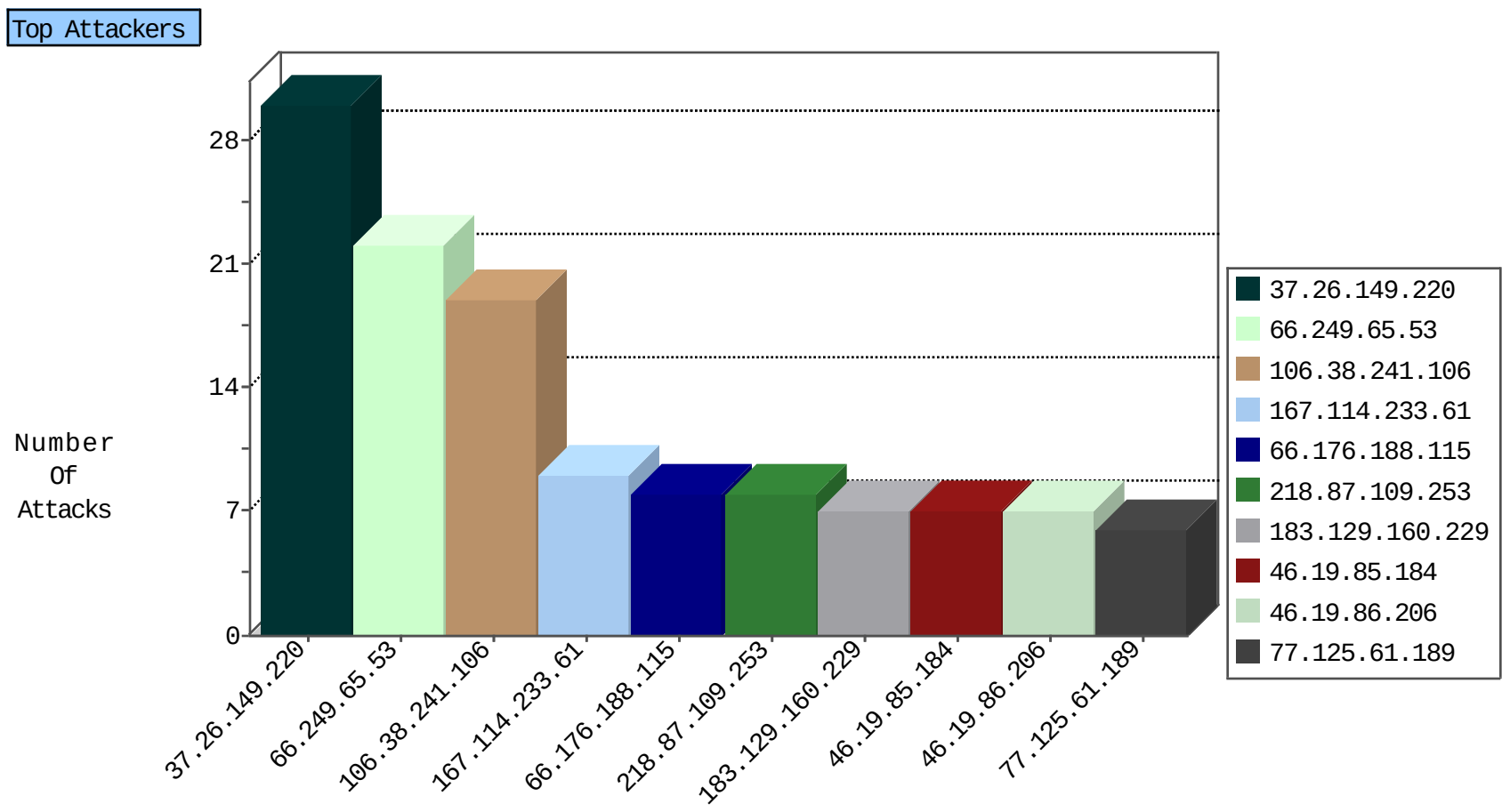
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-04-2016-02:04:06 to 10-04-2016-03:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
110.154.170.226	China	147.237.76.197	e.himush.idf.il	Black List	drop	1
60.191.221.175	China	147.237.0.34	tikshuv.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
223.85.106.194	China	147.237.76.86	navy.idf.il	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1
94.102.49.193	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1

10-04-2016-02:04:06 to 10-04-2016-03:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	17
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
162.210.196.129	United States	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-04-2016-02:04:06 to 10-04-2016-03:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	1
218.87.109.253	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
24.39.95.126	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
180.213.5.205	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
89.163.224.115	147.237.8.14	Germany	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
89.163.224.115	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
109.236.86.32	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
89.163.224.115	147.237.8.27	Germany	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
89.163.224.115	147.237.0.34	Germany	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
79.41.100.24	147.237.77.205	Italy	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1

10-04-2016-02:04:06 to 10-04-2016-03:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.53	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
37.26.149.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
66.176.188.115	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.206	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
37.26.149.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.149.220	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.125.61.189	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
167.114.233.61	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.155	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
5.22.134.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.249.69.146	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
167.114.233.61	France	147.237.77.216	dover.idf.il	SYN Attack		monitor	3
176.13.233.222	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.49	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.253.138.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
187.61.122.119	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
37.26.146.229	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	2
138.246.253.19	Germany	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
183.129.160.229	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
85.64.36.172	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
191.241.39.114	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.26.146.229	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
183.129.160.229	China	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
141.212.122.109	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.26.149.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
183.129.160.229	China	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
2.53.5.153	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
167.114.233.61	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
88.57.44.81	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
198.20.69.74	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.26.146.229	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
183.129.160.229	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
141.212.122.110	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.26.149.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
183.129.160.229	China	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.9.17.118	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
167.114.233.61	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
109.67.204.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
183.129.160.229	China	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	1
37.26.149.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
185.3.147.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
172.56.34.77	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
213.57.240.109	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
37.26.148.155	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
183.129.160.229	China	147.237.77.205	prisha.idf.il	drop	SAM rule	drop	1
37.26.149.220	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

10-04-2016-02:04:06 to 10-04-2016-03:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.139.224.198	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	3
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
176.13.246.216	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
100.45.246.219	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/71552.pdf	Block	1
2.53.51.67	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
150.70.188.169	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/69499.pdf	Block	1
204.79.180.50	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
73.13.96.153	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
40.77.167.30	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
173.231.185.150	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/admin/i18n/readme.txt	Block	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/71568.pdf	Block	1
173.231.185.150	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/admin/i18n/readme.txt	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
46.19.85.184	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/69049.pdf	Block	1

10-04-2016-02:04:06 to 10-04-2016-03:04:06