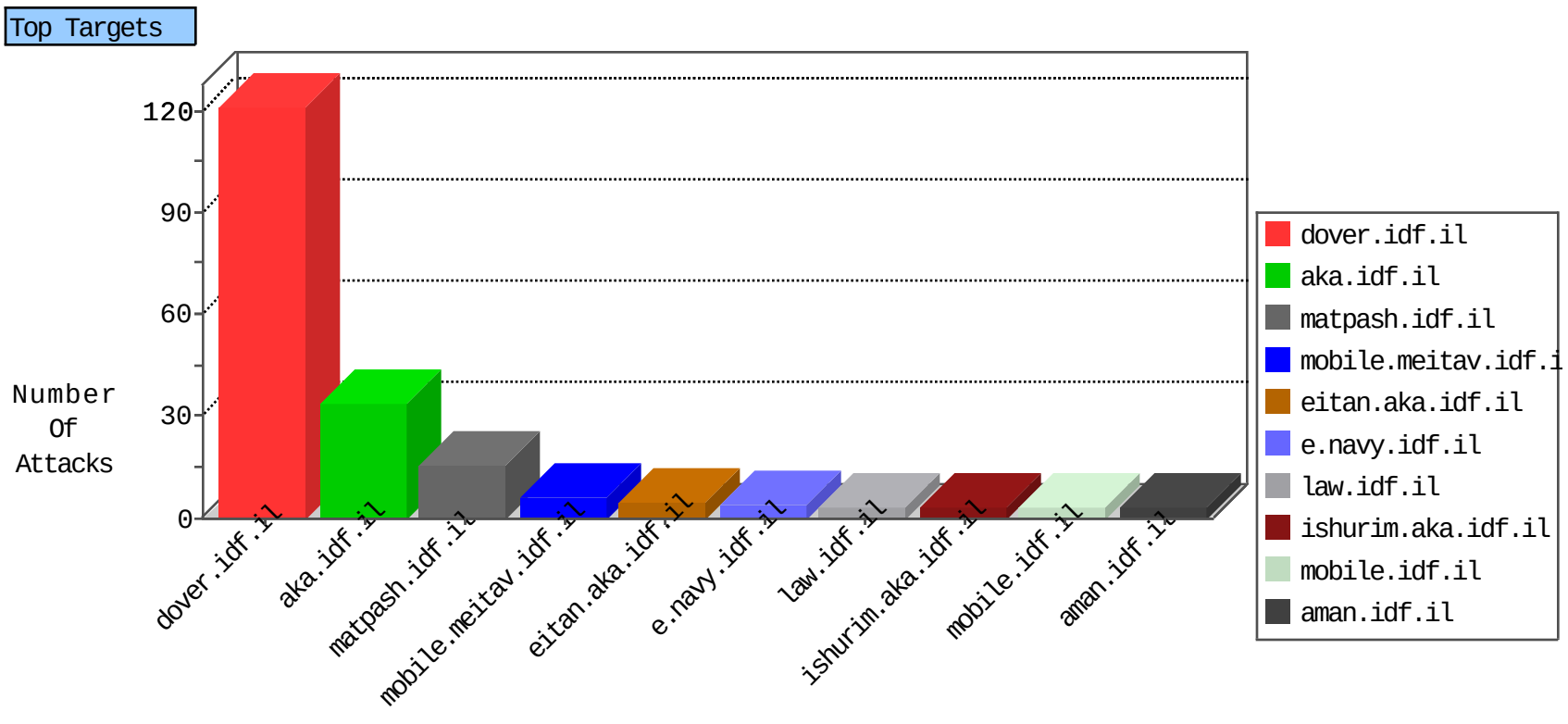
10-04-2016-03:04:06 to 10-04-2016-04:04:06

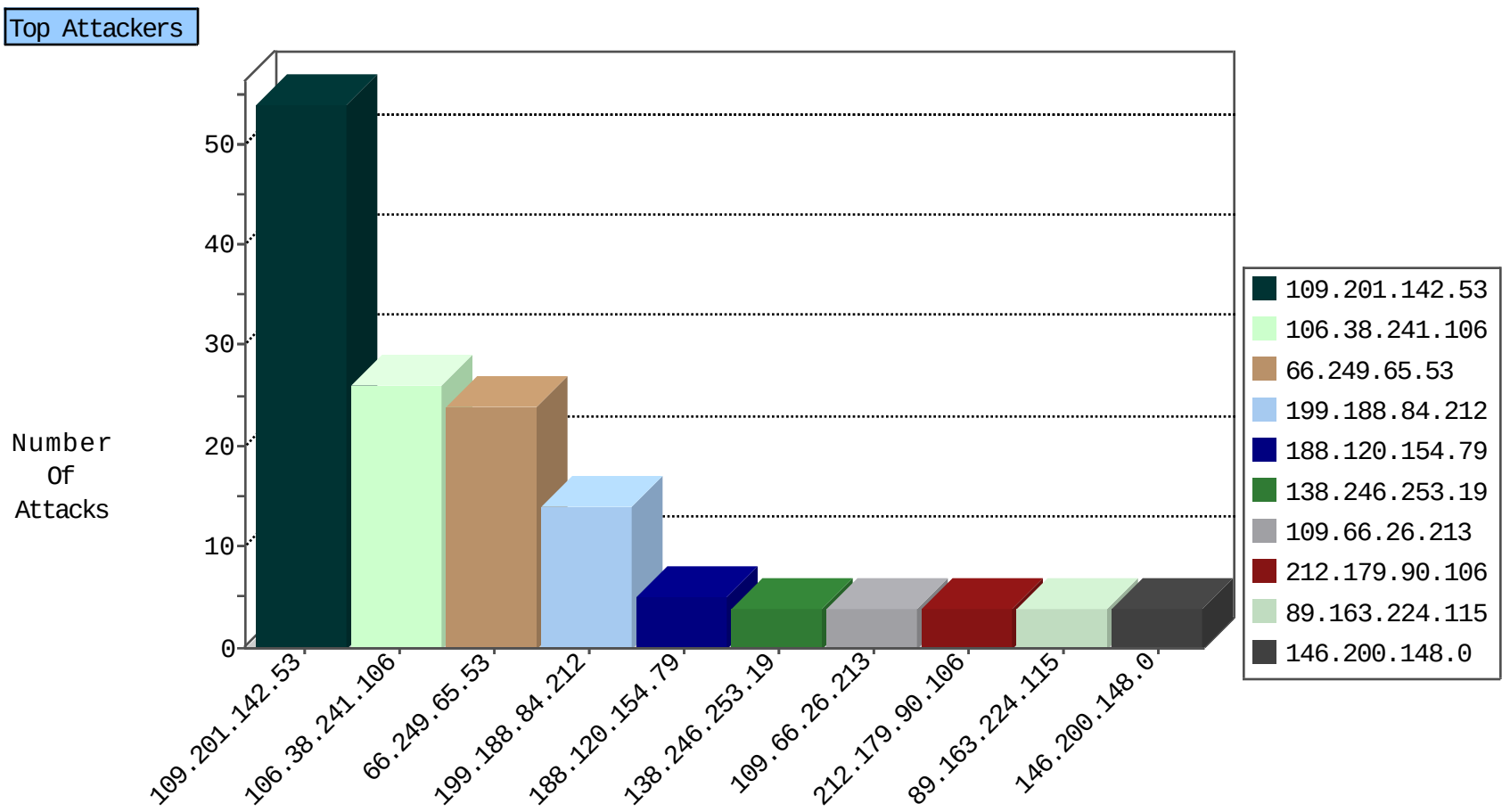
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.201.142.53	Netherlands	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	22
109.201.142.53	Netherlands	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	16
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
195.62.53.168	Russian Federation	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
36.71.40.212	Indonesia	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
188.138.26.214	Germany	147.237.76.201	e.atal.idf.il	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
188.138.26.214	Germany	147.237.76.202	e.halag.idf.il	Black List	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	13
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	12
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
109.201.142.53	Netherlands	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

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

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
146.200.148.0	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
146.200.148.0	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
89.163.224.115	147.237.77.233	Germany	atal.idf.il	ET SCAN Potential SSH Scan	1
89.163.224.115	147.237.77.121	Germany	e.navy.idf.il	ET SCAN Potential SSH Scan	1
85.93.5.70	147.237.77.233	United Arab Emirates	atal.idf.il	ET SCAN Potential SSH Scan	1
14.152.59.11	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
177.4.200.183	147.237.76.39	Brazil	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
128.199.76.253	147.237.76.197	Singapore	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
89.163.224.115	147.237.77.234	Germany	halag.idf.il	ET SCAN NMAP -sS window 1024	1
89.163.224.115	147.237.77.205	Germany	prisha.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	147.237.0.17	Turkey	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.91.21	147.237.77.74	Ukraine	law.idf.il	ET SCAN NMAP -sS window 1024	1
177.4.200.183	147.237.76.39	Brazil	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
177.4.200.183	147.237.76.39	Brazil	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
125.65.82.44	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

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

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	24
199.188.84.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.66.26.213	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.32.179.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.154.79	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.87.168.146	Ukraine	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.177.159.45	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
5.122.219.247	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
81.199.120.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
5.122.219.247	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
207.46.13.58	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
157.55.39.170	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.149	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
188.120.154.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.201.98	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.211	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.49	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.108	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
138.246.253.19	Germany	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.212	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.96	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
201.179.59.20	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.111	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
138.246.253.19	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.103	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
138.246.253.19	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
68.81.206.98	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.82	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.104	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
23.121.34.174	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.139.71	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
138.246.253.19	Germany	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.31	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.112	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.107	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.201.142.53	Netherlands	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.201.142.53	Block	27
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.41	Block	1
204.79.180.35	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
68.180.229.178	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
109.201.142.53	Netherlands	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
217.132.181.129	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
174.16.57.102	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/general/default.asp	Block	1
66.249.76.52	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
195.62.53.168	Russian Federation	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to gmail.com/engine/log.txt	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
84.229.33.230	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
54.169.226.39	Singapore	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/web-console/serverinfo.jsp	Block	1
201.214.111.14	Chile	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.77	Block	1

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