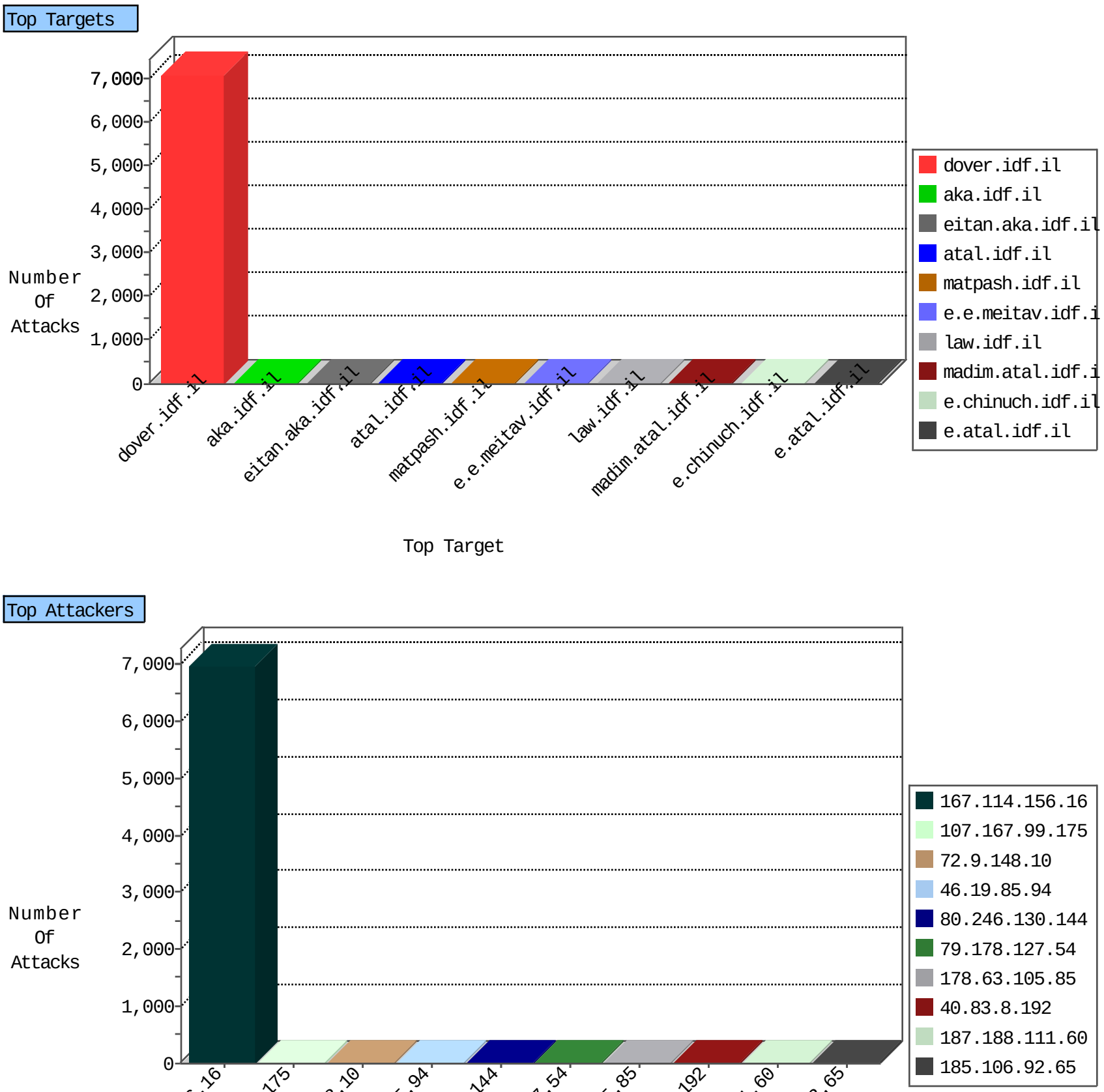
03-13-2016-05:04:04 to 03-13-2016-06:04:04

IDF Under Attack Daily Report



03-13-2016-05:04:04 to 03-13-2016-06:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	8455
184.105.139.80	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1

03-13-2016-05:04:04 to 03-13-2016-06:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
164.132.161.21	Italy	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.7	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.56	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-13-2016-05:04:04 to 03-13-2016-06:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.246.130.144	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
218.246.0.97	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
23.96.109.87	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
218.57.11.7	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
40.83.8.192	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.65	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
40.83.8.192	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.65	147.237.76.31		nakchal.idf.il	ET SCAN Potential SSH Scan	1
40.83.8.192	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.65	147.237.0.19		madim.atal.idf.il	ET SCAN Potential SSH Scan	1
40.83.8.192	147.237.72.217	United States	e.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.76.201		e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
40.83.8.192	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
114.34.30.193	147.237.8.27	Taiwan	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.246.0.97	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
23.96.109.87	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
103.9.163.151	147.237.76.38	Australia	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
218.57.11.7	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
80.82.65.82	147.237.77.216	Netherlands	dover.idf.il	ET WEB_SERVER Poison Null Byte	1
218.57.11.7	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
187.188.111.60	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
40.83.8.192	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.65	147.237.76.39		mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
40.83.8.192	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.65	147.237.0.33		idf.il	ET SCAN Potential SSH Scan	1
40.83.8.192	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.65	147.237.0.19		madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
40.83.8.192	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.76.197		e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
40.83.8.192	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
103.9.163.151	147.237.76.38	Australia	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1

03-13-2016-05:04:04 to 03-13-2016-06:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3344
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	86
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	27
107.167.99.175	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
79.178.127.54	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
80.246.130.144	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	4
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.i	drop	SAM rule	drop	4
46.19.85.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.130.144	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.29.78.38	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
79.179.21.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.35.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
2.52.164.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
95.86.88.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
71.167.34.127	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
184.105.247.247	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
187.188.111.60	Mexico	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
40.77.167.52	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
137.226.113.7	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
74.82.47.60	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
70.35.197.33	United States	147.237.77.74	law.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
185.3.144.19	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
187.188.111.60	Mexico	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.83	United States	147.237.0.35	akaws.idf.il	drop		drop	1
198.20.69.74	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
70.35.197.33	United States	147.237.77.176	matpash.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
187.188.111.60	Mexico	147.237.0.33	idf.il	drop		drop	1
187.188.111.60	Mexico	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.103	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
187.188.111.60	Mexico	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
24.17.169.182	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.11	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
187.188.111.60	Mexico	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.207	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
71.190.255.85	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
187.188.111.60	Mexico	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.146.227	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.i	drop	SAM rule	drop	1

03-13-2016-05:04:04 to 03-13-2016-06:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.86.88.127	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20373-he/idfgdover.aspx	Block	1
68.180.230.152	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
37.237.162.74	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
157.55.39.193	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20367-he/idfgdover.aspx	Block	1
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	NULL Character in URL /english/organization/homefront/homefront2.stm[[#0]]	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
207.46.13.160	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/69421.pdf	Block	1
66.249.64.169	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/usercontrols/headerupper/	Block	1
217.69.133.246	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/kamlar/klali/default.asp	None	1
68.180.230.87	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	1
142.129.10.133	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.230.152	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	1
157.55.39.49	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1

03-13-2016-05:04:04 to 03-13-2016-06:04:04