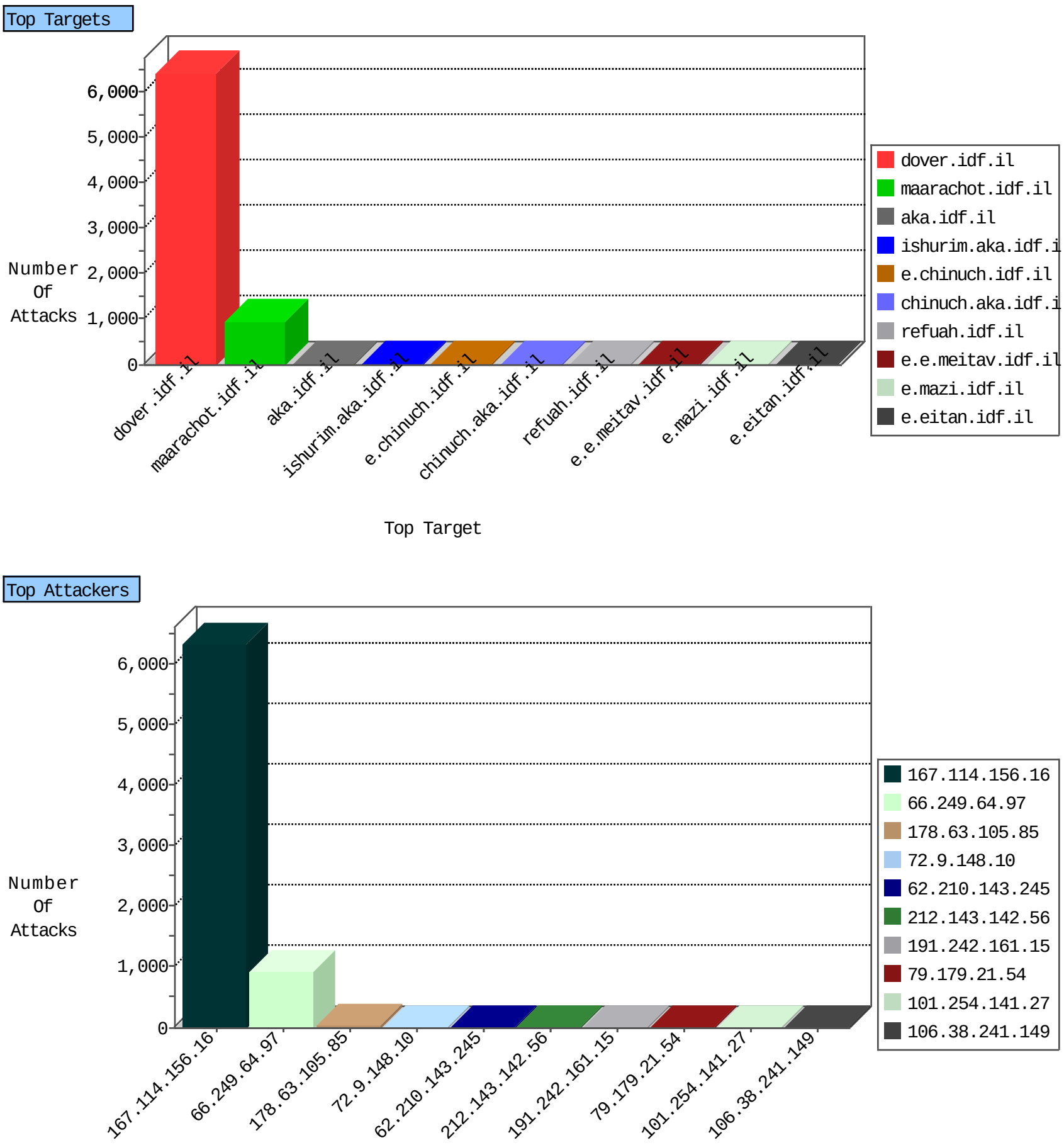
03-13-2016-04:04:01 to 03-13-2016-05:04:01

IDF Under Attack
Daily Report



03-13-2016-04:04:01 to 03-13-2016-05:04:01

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	9581
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3

03-13-2016-04:04:01 to 03-13-2016-05:04:01

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
144.76.8.132	Germany	147.237.72.167	ishurim.aka.idf.il	C1000074: HTTP: majestic bot	Block	2
51.255.162.164	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.8.132	Germany	147.237.77.226	www.chamatz.aka.idf.il	C1000074: HTTP: majestic bot	Block	2
62.210.97.48	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.129	Italy	147.237.76.31	nakchal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-13-2016-04:04:01 to 03-13-2016-05:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	934
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
183.179.235.195	147.237.8.28	Hong Kong	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.232.98.38	147.237.76.147		chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
101.254.141.27	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
101.254.141.27	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
101.254.141.27	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
61.216.84.147	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
104.232.98.38	147.237.76.147		chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
101.254.141.27	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
101.254.141.27	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
101.254.141.27	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 3072	1

03-13-2016-04:04:01 to 03-13-2016-05:04:01

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	2806
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	100
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	24
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.179.21.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
191.242.161.15	Brazil	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	5
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	5
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	5
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	5
178.63.18.196	Germany	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	3
141.8.142.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.10.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.210.143.245	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
62.210.143.245	France	147.237.77.233	atal.idf.il	drop	SAM rule	drop	2
62.210.143.245	France	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	2
62.210.143.245	France	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	2
62.210.143.245	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
144.76.8.132	Germany	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
191.242.161.15	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.117.3.104	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
94.242.195.186	Luxembourg	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
187.188.111.60	Mexico	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
151.80.31.129	Italy	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
75.126.221.55	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
207.46.13.87	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.117.3.104	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.38.241.149	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
187.188.111.60	Mexico	147.237.0.35	akaws.idf.il	drop		drop	1
178.63.105.85	Germany	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
207.241.229.224	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.120	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
187.188.111.60	Mexico	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.64.114.228	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.208	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.234	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
41.34.178.189	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.64.114.228	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.98	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.243	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.63.105.85	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1

03-13-2016-04:04:01 to 03-13-2016-05:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.0.115.141	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
87.71.9.228	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
146.115.59.132	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19667-he/idfgdover.aspx	Block	1
207.241.229.225	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/מאיר שחמון.aspx	Block	1
87.71.9.228	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
173.247.228.10	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1774	Block	1
213.57.149.132	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
64.134.178.126	United States	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
173.247.228.10	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
68.180.228.151	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
213.57.149.132	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
107.170.171.157	United States	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 107.170.171.157	Block	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
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
69.121.153.40	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
107.170.171.157	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-13104-en/dover.aspx	Block	1

03-13-2016-04:04:01 to 03-13-2016-05:04:01