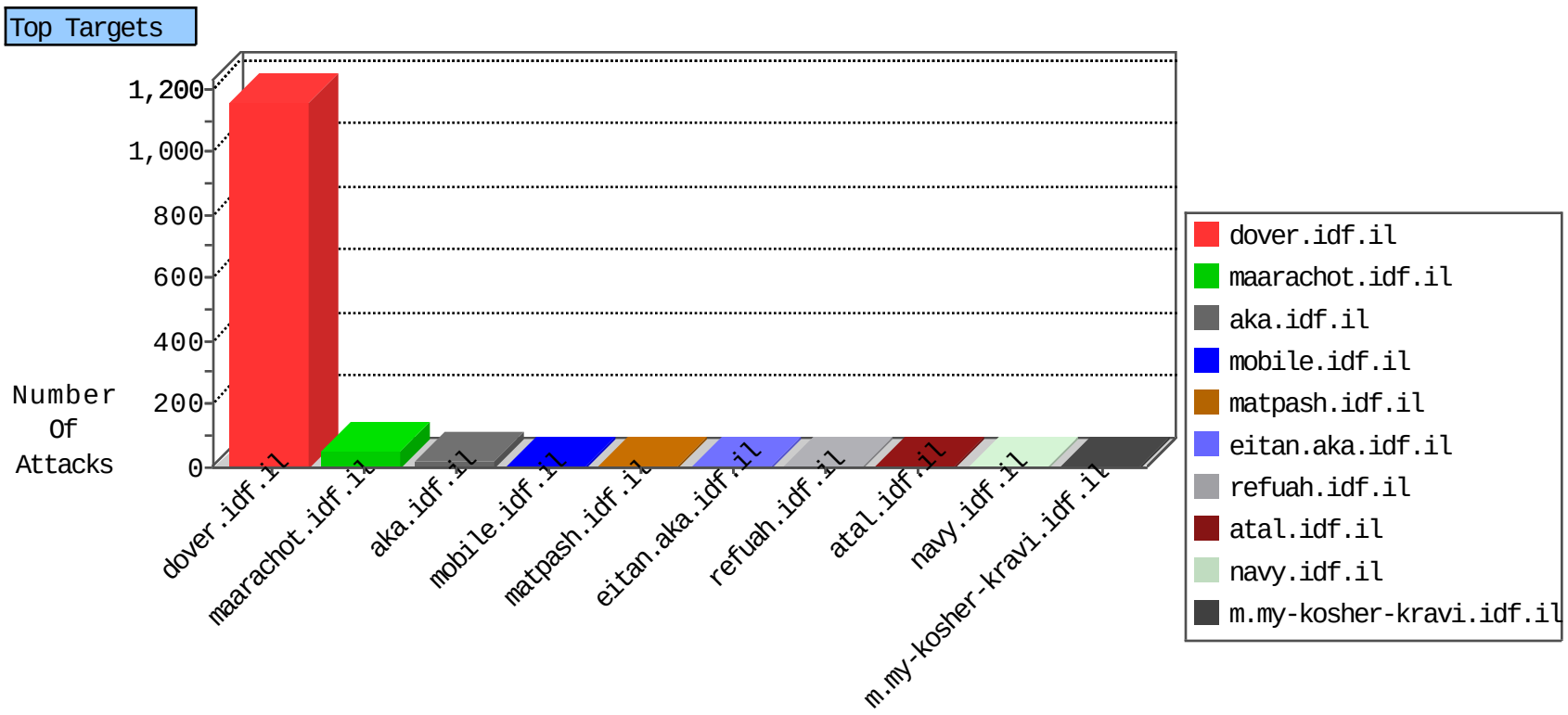
01-01-2016-05:04:00 to 01-01-2016-06:04:00

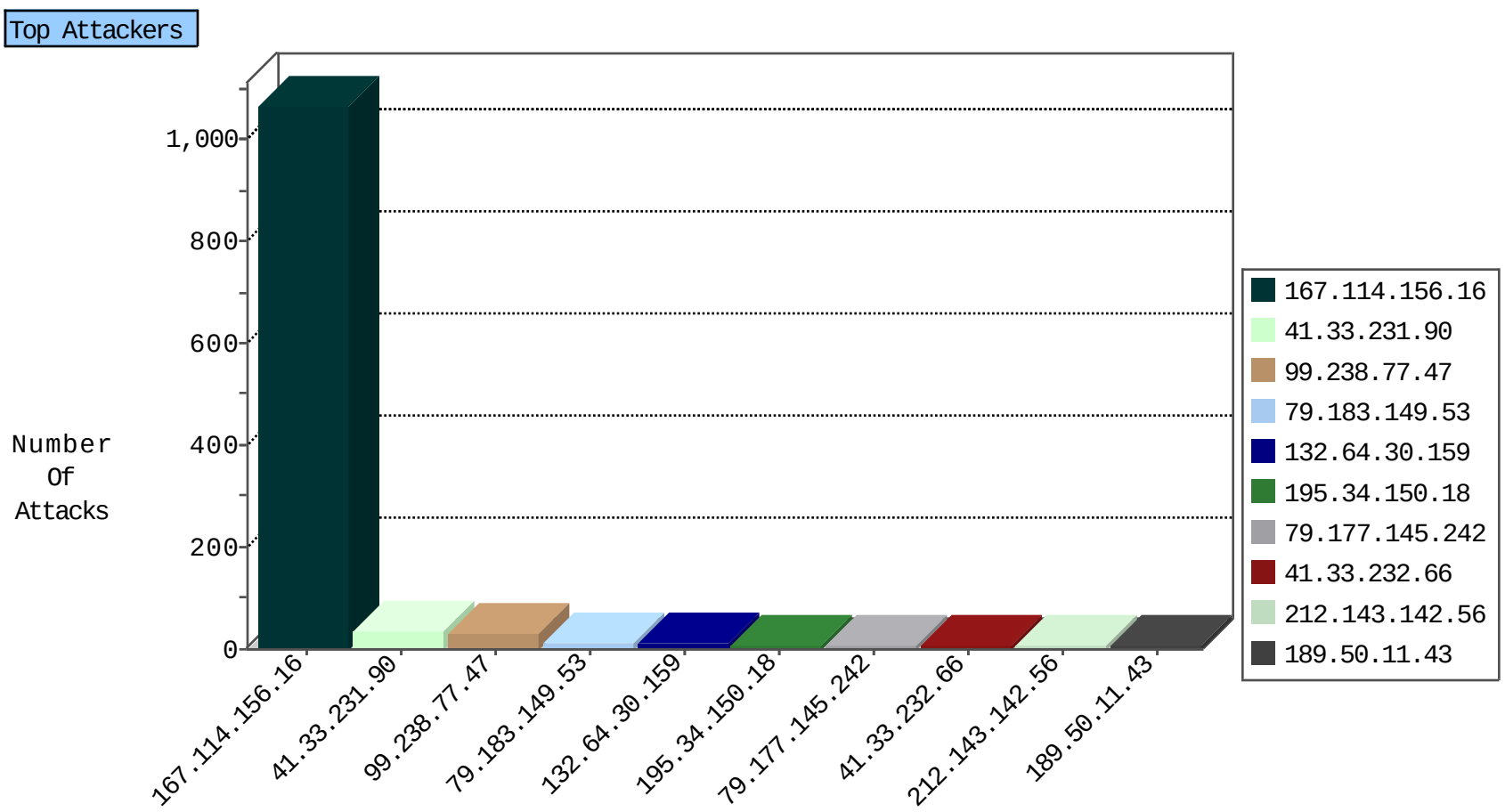
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-01-2016-05:04:00 to 01-01-2016-06:04:00

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	3126
66.249.64.191	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	31
180.97.106.161	China	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.161	China	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
146.185.239.100	Russian Federation	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1

01-01-2016-05:04:00 to 01-01-2016-06:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
185.130.5.224		147.237.77.226	www.chamatz.aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1

01-01-2016-05:04:00 to 01-01-2016-06:04:00

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
180.153.104.125	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
80.34.149.120	147.237.77.179	Spain	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
61.155.203.54	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
58.137.231.190	147.237.0.33	Thailand	idf.il	ET SCAN NMAP -sS window 1024	1
189.50.11.43	147.237.76.197	Brazil	e.himush.idf.il	ET SCAN Potential SSH Scan	1
189.50.11.43	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Potential SSH Scan	1
189.50.11.43	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.239	147.237.77.121		e.navy.idf.il	ET SCAN Potential SSH Scan	1
180.153.104.125	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
80.34.149.120	147.237.77.179	Spain	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
61.155.203.54	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
61.155.203.54	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
189.50.11.43	147.237.72.167	Brazil	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
189.50.11.43	147.237.0.19	Brazil	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.239	147.237.77.170		maarachot.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.239	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

01-01-2016-05:04:00 to 01-01-2016-06:04:00

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	36
99.238.77.47	Canada	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
132.64.30.159	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
79.183.149.53	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.177.145.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
199.30.25.213	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
87.68.51.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.132.0.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
45.55.53.138		147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.86.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
149.78.102.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.142.165.232	Israel	147.237.77.233	atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
204.12.251.37	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.248	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.154.146.225	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
146.185.239.102	Russian Federation	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
72.65.52.24	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.72	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.18	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.28.173.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
199.30.25.150	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
149.78.102.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
72.69.229.93	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.110	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.84	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
24.26.253.10	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
199.30.25.150	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.36	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.118	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.104	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
65.55.210.150	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
65.55.210.150	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

01-01-2016-05:04:00 to 01-01-2016-06:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.165.12	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 85.64.165.12	Block	2
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
149.88.140.93	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
173.245.81.49	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
65.75.122.147	Bahamas	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
74.82.47.4	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
85.250.208.38	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/xmlrpc.php	Block	1
65.75.122.147	Bahamas	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
217.132.136.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.180.186.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/13696.jpg	Block	1
104.172.142.227	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
80.246.136.162	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 80.246.136.162 (Unknown SSL Session)	None	1
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_id.20.8afc=e195ab7a512444f4.1428323478.8.1451619075.1451619075.;	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13974-en/dover.aspx&bw=1	Block	1
173.245.81.40	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
85.64.165.12	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method W8GI95R9OrZpGI44YM3nU0iOEwn7thnV0D2jKvCdHXwVB2LZROnbHh8sAFhQwgcHpkMO2DojGf%26s%3D1%22%5D; in URL _pk_id.20.8afc=e195ab7a512444f4.1428323478.8.1451619075.1451619075.	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1

01-01-2016-05:04:00 to 01-01-2016-06:04:00