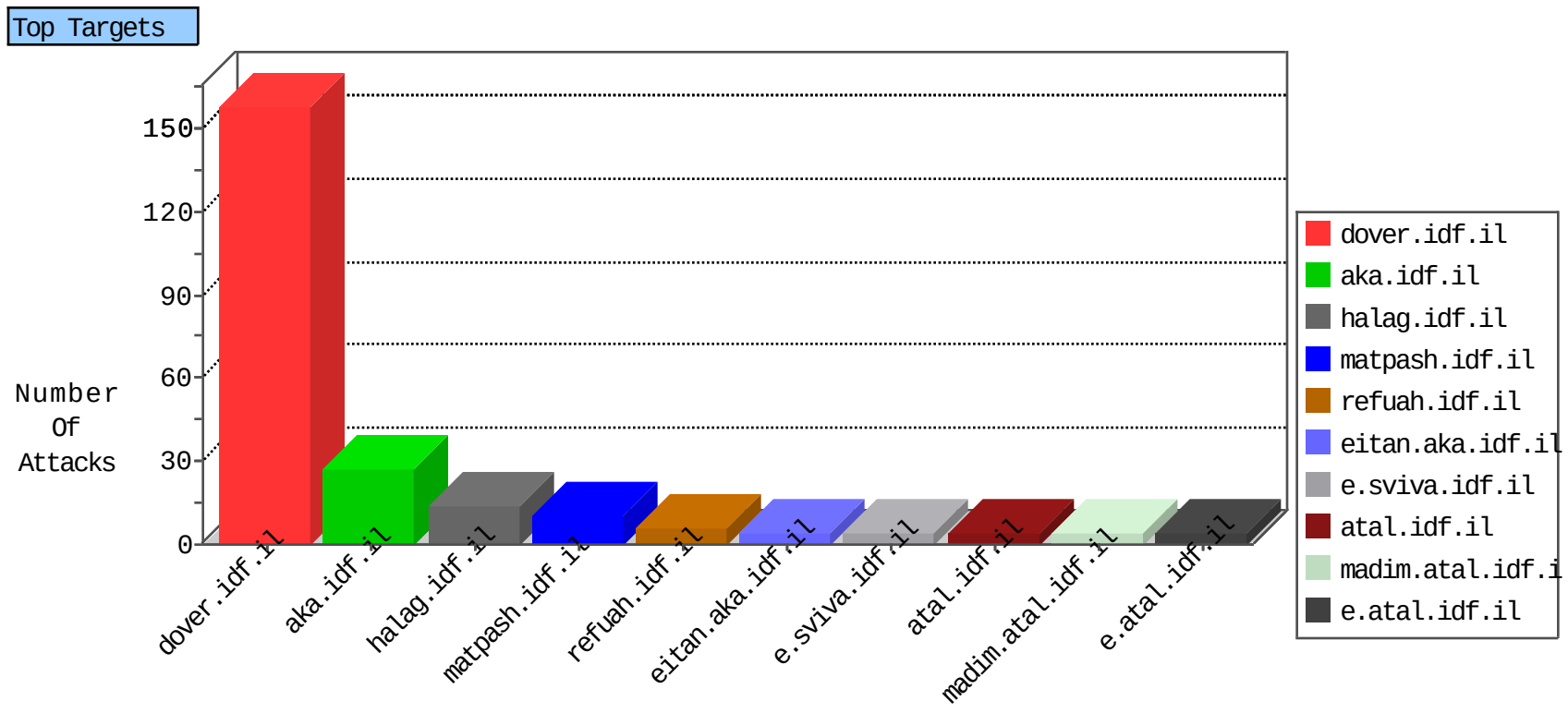
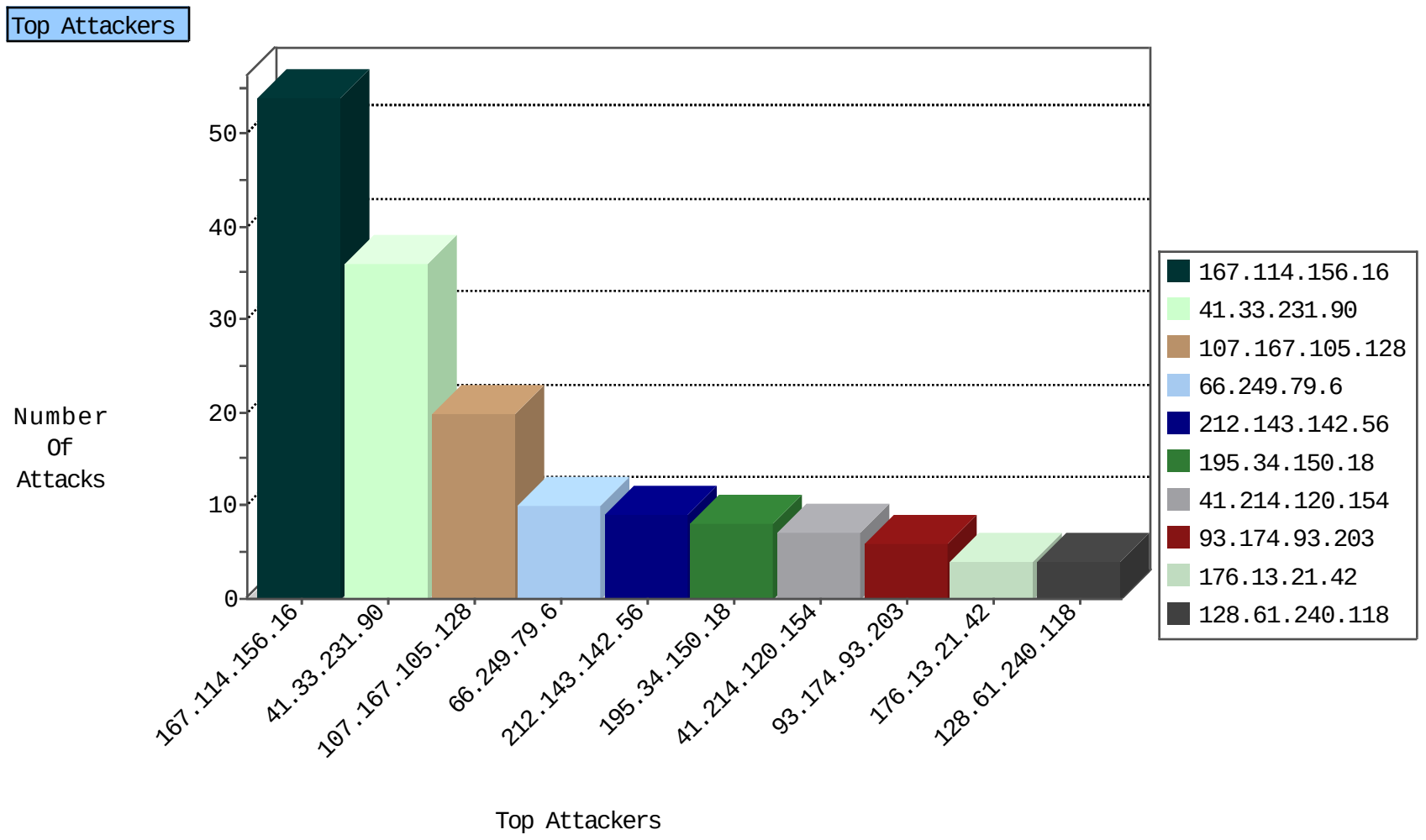
01-09-2016-04:04:07 to 01-09-2016-05:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



01-09-2016-04:04:07 to 01-09-2016-05:04:07

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	1253
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
115.239.228.10	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Http	drop	2
31.148.220.74	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
124.77.9.103	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
14.112.121.242	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

01-09-2016-04:04:07 to 01-09-2016-05:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-09-2016-04:04:07 to 01-09-2016-05:04:07

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
168.62.238.153	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.203	147.237.76.39	Netherlands	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
93.174.93.203	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
58.253.96.122	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 3072	1
93.174.93.203	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.203	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.122	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 4096	1

01-09-2016-04:04:07 to 01-09-2016-05:04:07

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	34
107.167.105.128	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
85.65.244.157	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
176.13.21.42	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.154.226.90	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
46.19.85.148	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.241	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
201.216.228.101	Argentina	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.120.79.141	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
93.174.93.203	Netherlands	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
66.147.244.138	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.120	United States	147.237.0.35	akaws.idf.il	drop		drop	1
37.26.147.198	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.192	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.61.240.118	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.57.0.231	Netherlands	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
24.241.18.212	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.157	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.108	United States	147.237.0.33	idf.il	drop		drop	1
184.105.247.199	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.200	United States	147.237.0.33	idf.il	drop		drop	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.130.231.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
31.168.67.217	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.158	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.61.240.118	United States	147.237.0.33	idf.il	drop		drop	1
216.218.206.116	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.10	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.199	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.201	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.147	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.130.231.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
201.216.228.101	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.95	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
31.168.67.217	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.158	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.61.240.118	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
218.22.211.69	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.42	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.220	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
14.211.74.211	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.148	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

01-09-2016-04:04:07 to 01-09-2016-05:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.214.120.154	Senegal	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.214.120.154	Block	7
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	2
131.253.25.201	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	2
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	2
157.55.39.47	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shop/view.php	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58604&docid=73552	Block	1
40.77.167.4	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1
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	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chinuch/contact	Block	1
114.98.226.56	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 114.98.226.56	Block	1
50.62.176.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
184.105.247.196	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
40.77.167.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 40.77.167.42	Block	1
207.46.13.121	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	1
114.98.226.56	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1570-ar/idfg.aspx/trackback/	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/3098.jpg	Block	1
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	1
188.143.232.21	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.21	Block	1
81.1.147.212	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
40.77.167.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/jscss/23.0.835/css/b7ed5398-5c2d-4fd0-b336-14981e78e997	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/brothers/gallery	Block	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.69.38	Block	1
17.138.58.206	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
188.143.232.21	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
157.55.39.47	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
37.48.80.101	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	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
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
50.62.176.49	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59329&docid=64979	Block	1

01-09-2016-04:04:07 to 01-09-2016-05:04:07