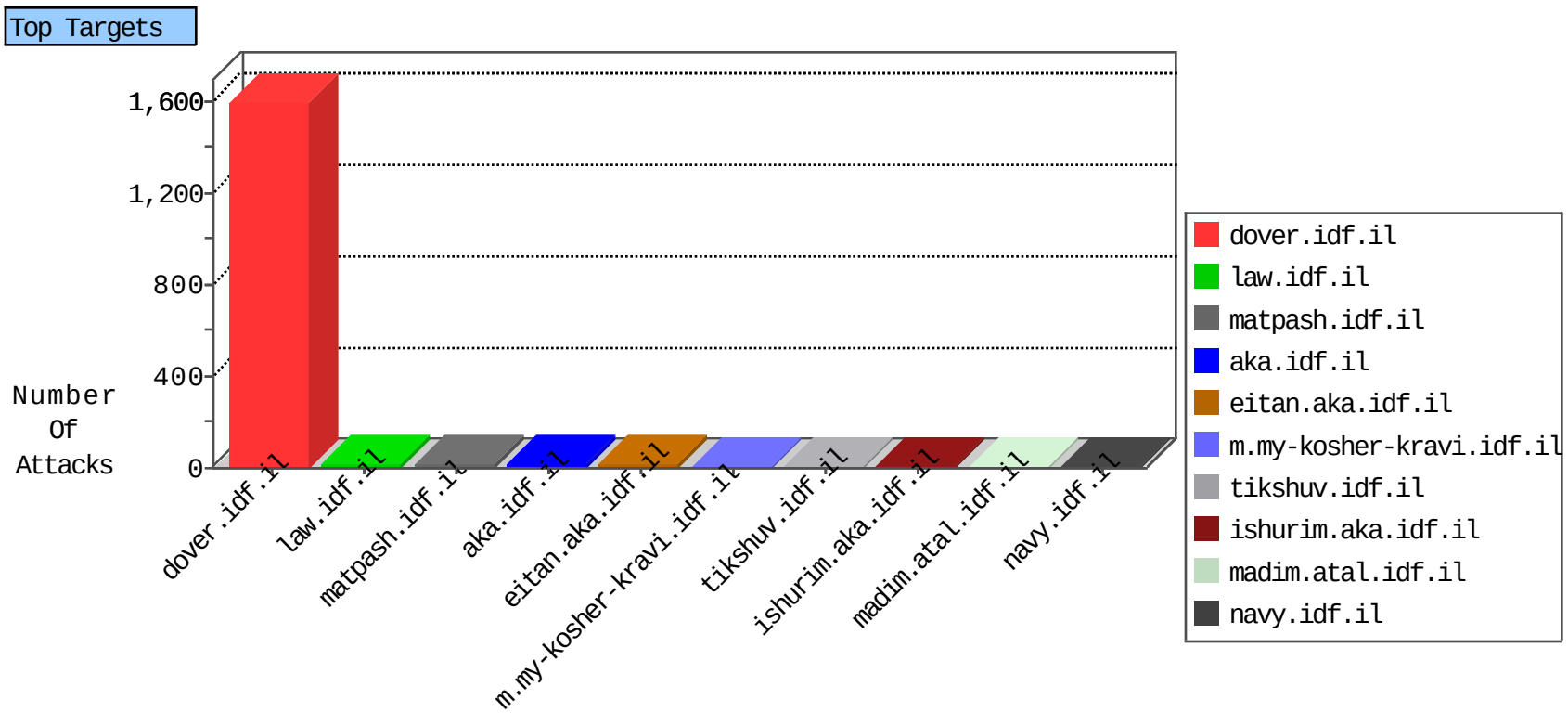
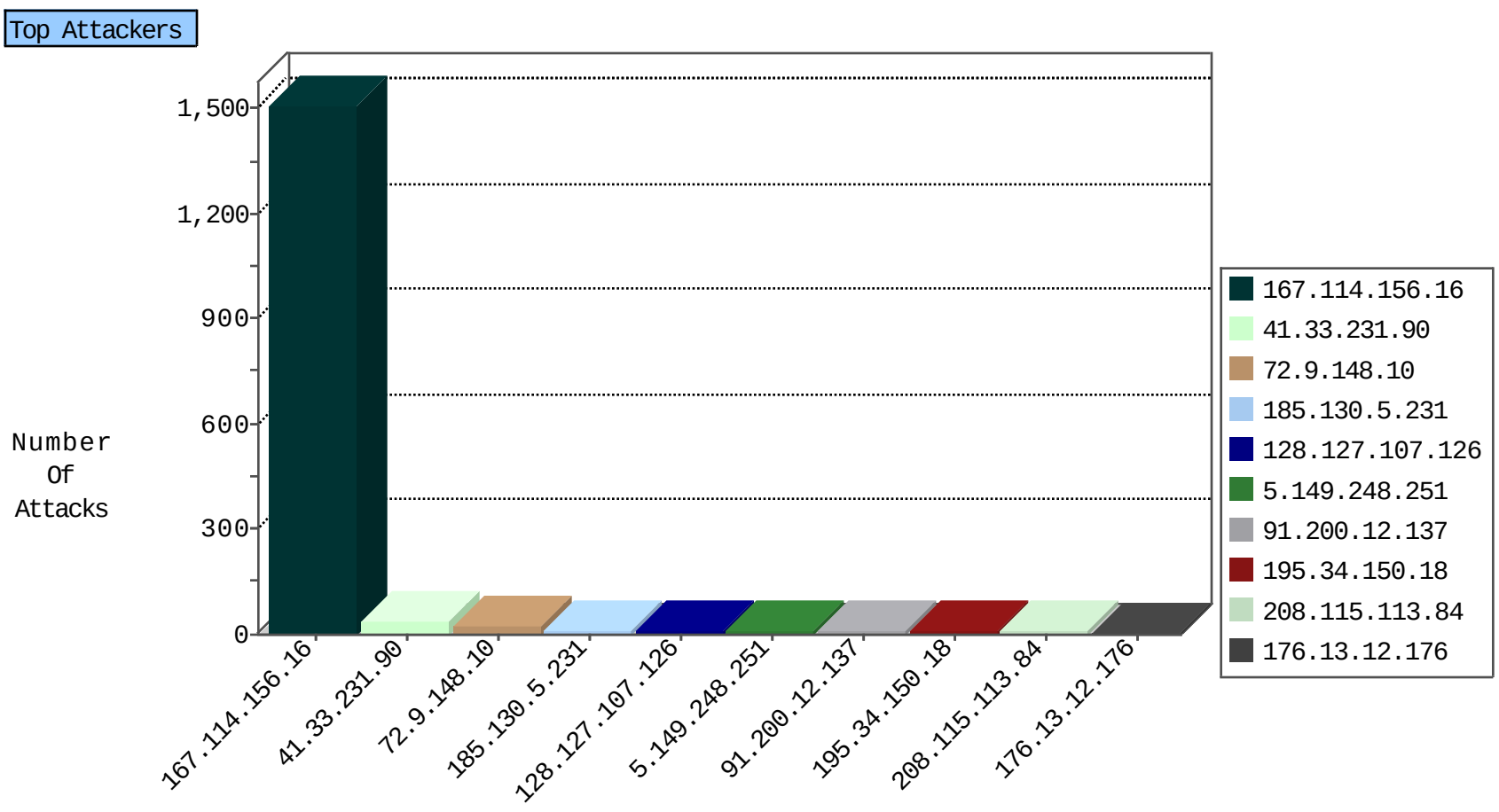
01-02-2016-06:04:05 to 01-02-2016-07:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-02-2016-06:04:05 to 01-02-2016-07:04:05

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	3272
74.91.124.204	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

01-02-2016-06:04:05 to 01-02-2016-07:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-02-2016-06:04:05 to 01-02-2016-07:04:05

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
185.130.5.224	147.237.72.167		ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
118.68.179.139	147.237.72.217	Vietnam	e.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
5.149.248.251	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
210.117.121.60	147.237.0.16	Korea, Republic of	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
209.126.116.147	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.231	147.237.72.167		ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.224	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 1024	1
120.146.199.131	147.237.0.34	Australia	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.76.31		nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
5.149.248.251	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
210.117.121.60	147.237.0.16	Korea, Republic of	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
209.126.116.147	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.7	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

01-02-2016-06:04:05 to 01-02-2016-07:04:05

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
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
128.127.107.126	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	8
91.200.12.137	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
157.55.2.154	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.137	Ukraine	147.237.77.216	dover.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
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
199.30.25.218	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
65.55.210.38	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.244.126	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
168.150.125.32	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
204.79.180.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
204.79.180.229	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.130.5.231		147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.0.33	idf.il	drop	SAM rule	drop	1
173.236.152.135	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.168	United States	147.237.0.35	akaws.idf.il	drop		drop	1
185.130.5.231		147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
5.149.248.251	Netherlands	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.115	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
193.171.202.150	Austria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.130.5.231		147.237.8.24	e.lifestyle.idf.il	drop	SAM rule	drop	1
178.62.162.228	United Kingdom	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.169	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.231		147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
5.149.248.251	Netherlands	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.219	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.146	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.231		147.237.8.27	e.madim.atal.idf.il	drop	SAM rule	drop	1
5.149.248.251	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.75	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.169	United States	147.237.0.35	akaws.idf.il	drop		drop	1
185.130.5.231		147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
5.149.248.251	Netherlands	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.224		147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.154.146.225	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
61.135.190.198	China	147.237.0.33	idf.il	drop		drop	1
185.130.5.231		147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
5.149.248.251	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.78	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.172	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.90	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.231		147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.12.176	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.12.176	None	4
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
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	2
66.249.78.184	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
61.135.190.72	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/1.he/langstyle.css	Block	1
157.55.39.137	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/shared/usercontrols/headerupper/	Block	1
86.47.80.145	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
61.135.190.200	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/reset.css	Block	1
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/general/eitan.aspx	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=58623&docid=77022	Block	1
61.135.190.197	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
176.13.12.176	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
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
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/3170.pdf	Block	1
52.90.147.148	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
141.212.122.160	United States	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 147.237.0.19/	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	1
61.135.190.197	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/datepicker.css	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId59034 in www.aka.idf.il/main/rabanut/general.aspx	None	1
61.135.190.69	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/text.css	Block	1
141.212.122.160	United States	147.237.72.167	ishurim.aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.167/	Block	1
77.75.77.101	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
61.135.190.198	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/layoutdev.css	Block	1
185.106.94.74		147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/xmlrpc.php	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
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info13.asp	Block	1
61.135.190.71	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/nav.css	Block	1
148.251.21.227	Germany	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/14-he	Block	1
84.94.176.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
61.135.190.200	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	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
109.66.54.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1