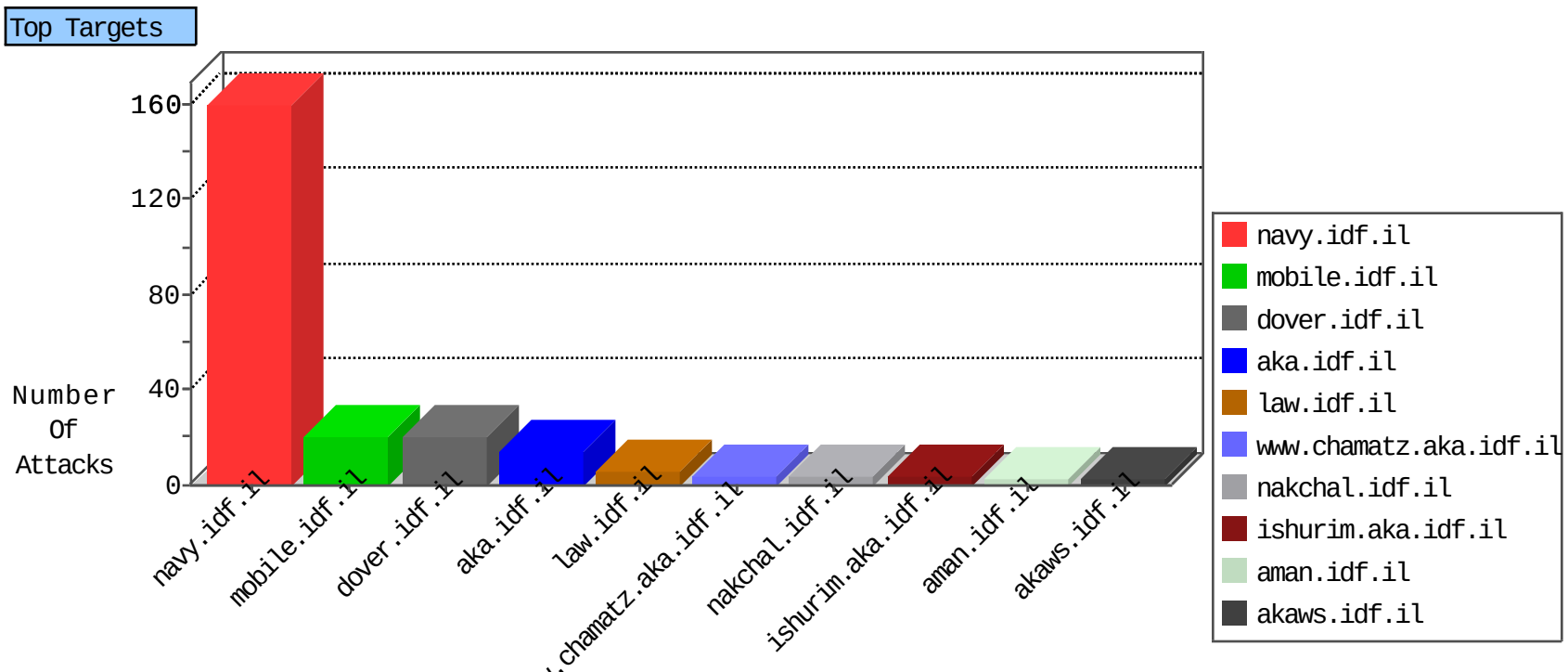
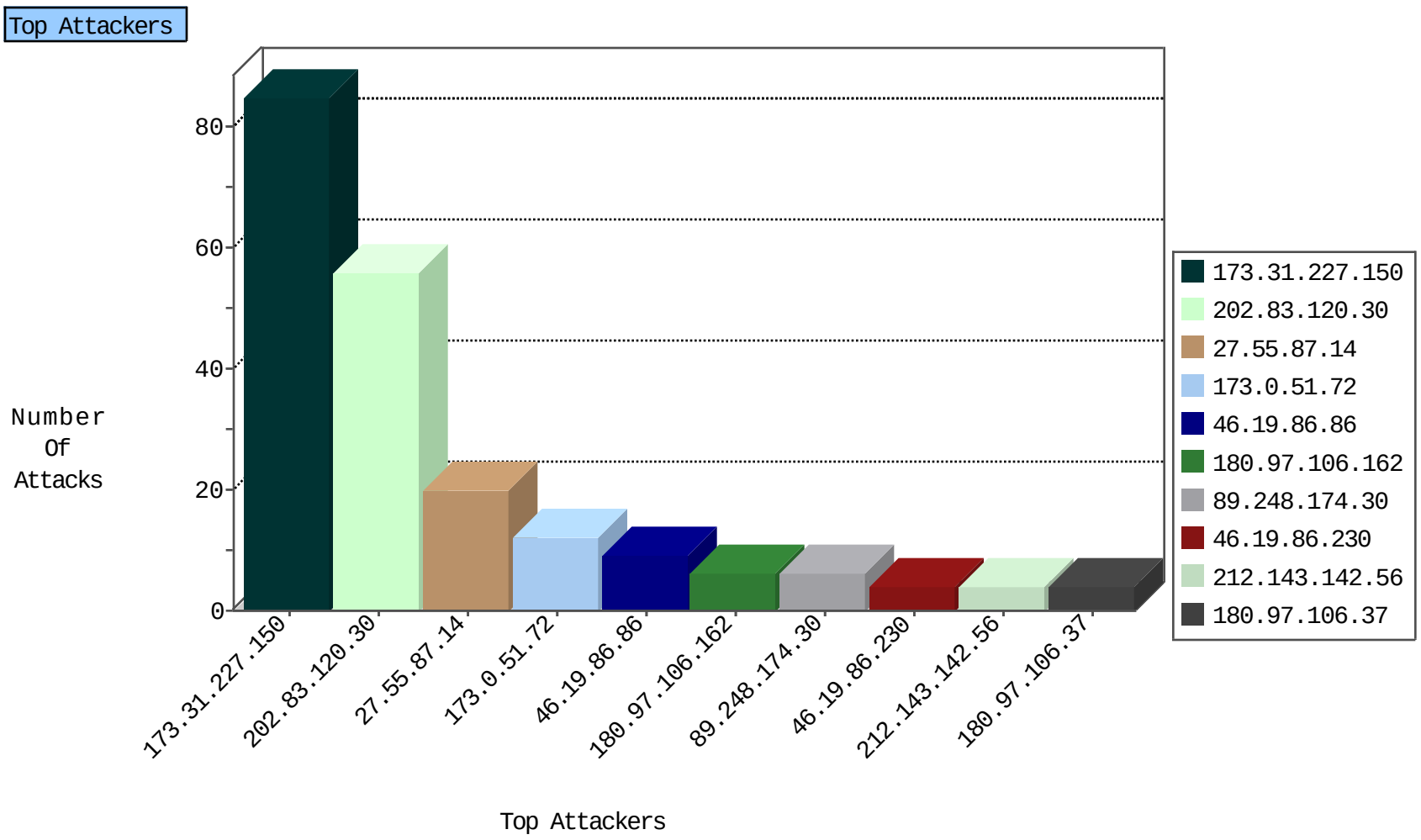
09-22-2016-04:04:04 to 09-22-2016-05:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-22-2016-04:04:04 to 09-22-2016-05:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
110.249.208.86	China	147.237.72.167	ishurim.aka.idf.il	DOSS-tcp-zero-seq	drop	1
45.32.205.187	Netherlands	147.237.76.197	e.himush.idf.il	Black List	drop	1
189.61.175.116	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
82.221.105.7	Iceland	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
110.249.208.86	China	147.237.0.16	my-kosher-kravi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
38.229.1.13	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1

09-22-2016-04:04:04 to 09-22-2016-05:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.210.239.204	Netherlands	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1

09-22-2016-04:04:04 to 09-22-2016-05:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
58.221.242.130	147.237.76.39	China	mobile.meitav.idf.il	GPL SCAN nmap TCP	2
212.86.219.134	147.237.77.74	Germany	law.idf.il	Tehila - Perl LWP with fake user agent	2
89.248.174.30	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.27.1.174	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.201.80	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
202.164.39.21	147.237.0.17	India	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
125.213.243.10	147.237.72.167	Thailand	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
115.47.12.162	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
89.248.174.30	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.30	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.30	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
64.137.168.128	147.237.76.31	Canada	nakchal.idf.il	ET SCAN Potential SSH Scan	1
41.160.222.18	147.237.77.121	South Africa	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.201.80	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.213.241	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
125.213.243.10	147.237.72.166	Thailand	aka.idf.il	ET SCAN NMAP -sS window 1024	1
93.190.90.226	147.237.77.216	Germany	dover.idf.il	ET SCAN Potential SSH Scan	1
89.248.174.30	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.30	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-22-2016-04:04:04 to 09-22-2016-05:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
27.55.87.14	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
173.31.227.150	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	18
173.31.227.150	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	18
173.31.227.150	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	17
173.31.227.150	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
173.31.227.150	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
202.83.120.30	Indonesia	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	12
202.83.120.30	Indonesia	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	11
202.83.120.30	Indonesia	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
202.83.120.30	Indonesia	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
202.83.120.30	Indonesia	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.86.86	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
173.0.51.72	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
173.0.51.72	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.230	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.230	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
173.0.51.72	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
141.212.122.29	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.117.107.241	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.100	United States	147.237.0.35	akaws.idf.il	drop		drop	1
173.0.51.72	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
141.212.122.31	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
115.28.218.121	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.85.219	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
173.0.51.72	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
141.212.122.30	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.52	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
198.20.69.74	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
171.120.27.219	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
115.28.218.121	China	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
141.212.122.30	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.59	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
173.0.51.72	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.19	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.67.97.222	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
173.0.51.72	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
141.212.122.30	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.60	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
173.0.51.72	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	alert	1
141.212.122.20	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.114	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.67.97.222	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.31	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
115.28.218.121	China	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
173.0.51.72	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1

09-22-2016-04:04:04 to 09-22-2016-05:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.210.239.204	Netherlands	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UncleTypesToIgnore	Block	2
180.94.113.57	Australia	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	2
180.97.106.37	China	147.237.76.30	himush.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/bamachane	Block	1
213.8.204.24	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
180.97.106.161	China	147.237.0.19	madim.atal.idf.il	Multiple NULL Character in Method from 180.97.106.161	Block	1
134.249.233.75	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
180.97.106.162	China	147.237.76.147	chinuch.aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
180.97.106.37	China	147.237.76.30	himush.idf.il	NULL Character in Method	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter utm_source in www.aka.idf.il/ishurim/main	None	1
213.8.204.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/xmlrpc.php	Block	1
180.97.106.161	China	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method	Block	1
180.97.106.162	China	147.237.76.147	chinuch.aka.idf.il	Distributed NULL Character in Method	Block	1
180.97.106.37	China	147.237.77.226	www.chamatz.aka.idf.il	Multiple Illegal Byte Code Character in Method from 180.97.106.37	Block	1
68.180.230.216	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1111-he/nakhal.aspx	Block	1
180.97.106.161	China	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
157.55.39.8	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
180.97.106.162	China	147.237.77.74	law.idf.il	Illegal Byte Code Character in Method	Block	1
180.97.106.37	China	147.237.77.226	www.chamatz.aka.idf.il	Multiple NULL Character in Method from 180.97.106.37	Block	1
124.73.5.134	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/default.aspx/trackback/	Block	1
180.97.106.162	China	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
180.97.106.162	China	147.237.77.74	law.idf.il	NULL Character in Method	Block	1
180.97.106.161	China	147.237.0.19	madim.atal.idf.il	Multiple Illegal Byte Code Character in Method from 180.97.106.161	Block	1
130.193.37.2	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
180.97.106.162	China	147.237.72.166	aka.idf.il	Distributed NULL Character in Method	Block	1

09-22-2016-04:04:04 to 09-22-2016-05:04:04