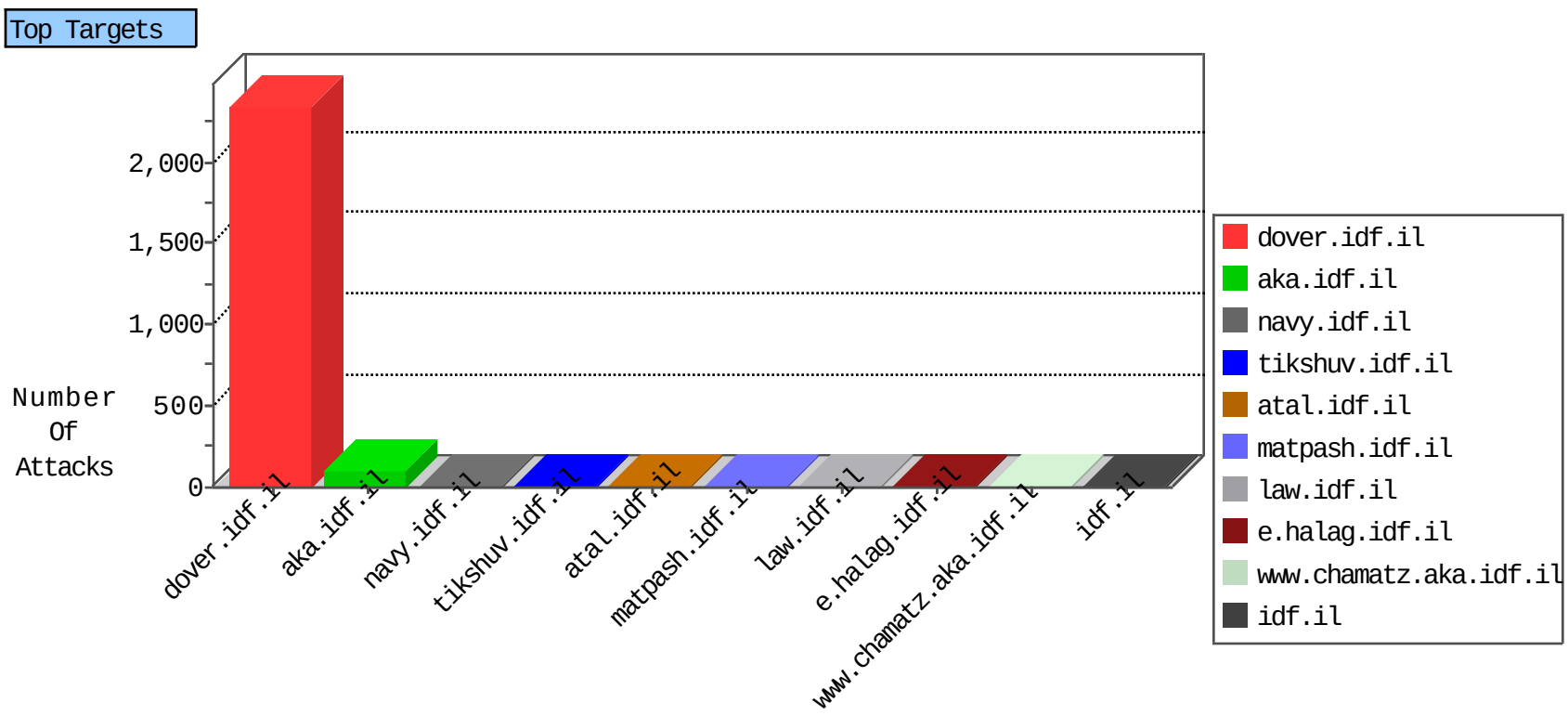
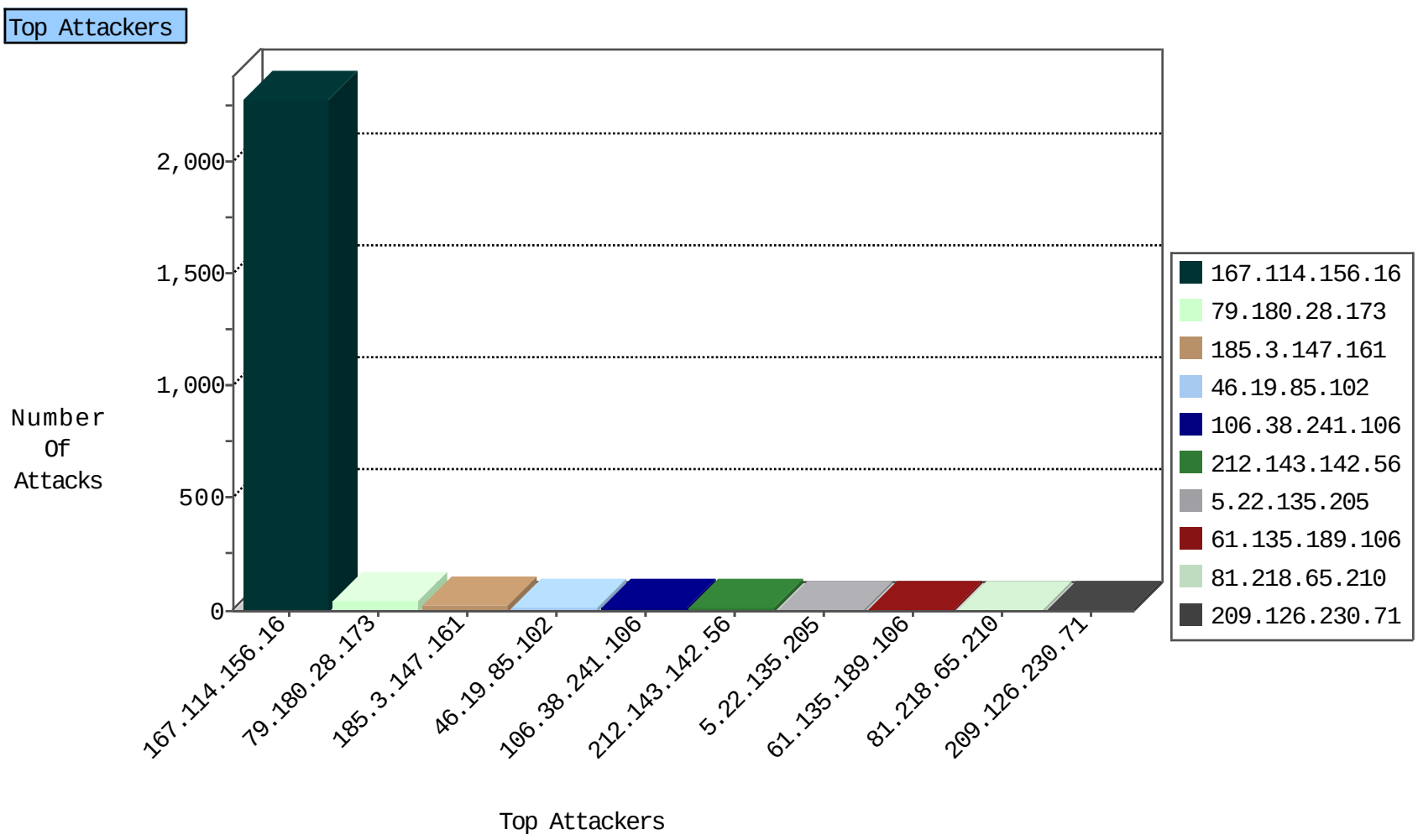
03-15-2016-01:07:33 to 03-15-2016-02:07:33

IDF Under Attack Daily Report





03-15-2016-01:07:33 to 03-15-2016-02:07:33

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	3539
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3

03-15-2016-01:07:33 to 03-15-2016-02:07:33

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
61.135.189.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2

03-15-2016-01:07:33 to 03-15-2016-02:07:33

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
64.233.172.163	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
164.39.11.198	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN NMAP -sS window 1024	1
147.175.16.71	147.237.0.34	Slovakia	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
104.44.133.108	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
23.252.161.191	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
212.98.164.237	147.237.0.19	Belarus	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
205.204.66.125	147.237.0.15	Canada	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.154.49.74	147.237.8.14	France	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.76.34	Sweden	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
147.175.16.71	147.237.0.34	Slovakia	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
104.44.133.108	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
218.246.0.97	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
93.113.125.12	147.237.8.27	Romania	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
212.98.164.237	147.237.0.35	Belarus	akaws.idf.il	ET SCAN Potential SSH Scan	1
205.204.66.125	147.237.0.33	Canada	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.154.49.74	147.237.77.170	France	maarachot.idf.il	ET SCAN Potential SSH Scan	1

03-15-2016-01:07:33 to 03-15-2016-02:07:33

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.3.147.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.102	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
79.180.28.173	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.180.28.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.180.28.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.180.28.173	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
5.22.135.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.28.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
213.55.105.112	Ethiopia	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
87.106.184.160	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	4
79.180.169.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.15.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
61.135.189.106	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.54.5.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.204	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
197.165.129.145	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.26	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
91.194.84.106	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
185.3.147.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
188.120.148.164	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.222	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.64.22.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
209.126.230.71	United States	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
5.29.44.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
172.56.21.81	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.214	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.115	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
188.120.148.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.223	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
118.193.163.150	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
209.126.230.71	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.29.44.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.215	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
118.193.163.150	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
209.126.230.71	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.218	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
72.152.235.137	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
209.126.230.71	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.210	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.143.38.222	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.219	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
77.125.4.197	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
209.126.230.71	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.211	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

03-15-2016-01:07:33 to 03-15-2016-02:07:33

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
79.180.28.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
24.86.36.186	Canada	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	2
37.26.148.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	2
38.111.147.88	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 38.111.147.88	Block	2
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
157.55.39.46	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.105	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/')	Block	1
41.68.161.204	Egypt	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
157.55.39.193	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.66.105	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1776	Block	1
88.108.80.88	United Kingdom	147.237.0.34	tikshuv.idf.il	Suspicious Response Code	Block	1
41.68.161.204	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
181.128.198.130	Colombia	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.33	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.69.33	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
62.74.7.53	Greece	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.230.189	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info.asp	Block	1
118.193.163.150	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
197.165.129.145	Egypt	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1

03-15-2016-01:07:33 to 03-15-2016-02:07:33